This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☒ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 477 570 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
12.05.1999 Bulletin 1999/19

(51) Int Cl.[6]: **G06F 1/00**

(21) Application number: **91114459.0**

(22) Date of filing: **28.08.1991**

(54) Security system for electronic printing systems

Sicherheitssystem für elektronische Drucksysteme

Système de sécurité pour systèmes d'impressions électroniques

(84) Designated Contracting States:
DE FR GB

(30) Priority: **28.09.1990 US 591330**

(43) Date of publication of application:
01.04.1992 Bulletin 1992/14

(60) Divisional application: **97116029.6 / 0 818 724**

(73) Proprietor: **XEROX CORPORATION**
Rochester New York 14644 (US)

(72) Inventors:
- **Rourke, John L.**
  Fairport, N.Y. 14450 (US)
- **Wing, Peter D.**
  Webster, N.Y. 14580 (US)
- **Ratcliffe, Jack F., II**
  Pittsford, N.Y. 14534 (US)
- **Vailliere, Paul J.**
  Fairport, N.Y. 14450 (US)

(74) Representative: **Grünecker, Kinkeldey,**
Stockmair & Schwanhäusser Anwaltssozietät
Maximilianstrasse 58
80538 München (DE)

(56) References cited:
EP-A- 0 366 425

- **SOFTWARE PRACTICE & EXPERIENCE. vol. 20, no. 5, May 1990, CHICHESTER GB pages 485 - 497; M.BISHOP: 'COLLABORATION USING ROLES'**
- **PROCEEDINGS, FJCC, 1987,OCT.25-29, INFOMART, DALLAS, TEXAS, P.421-426 L.J.FRAIM " SECURE OFFICE MANAGEMENT SYSTEM "**

EP 0 477 570 B1

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] The invention relates to electronic printers and printing systems, and to a security system for electronic printers and printing systems .

[0002] In particular, the invention relates to a security process for an electronic reprographic printer, comprising the steps of: providing a security administrator; providing a security profile with discrete security levels for different classes of users under the control of said security administrator; giving said administrator power to assign user identification numbers, and enable use of passwords by said users; providing user file security by assigning a non-removable security label to a user's files which prevents printing or displaying of said files without said security label.

[0003] Further, the invention also relates to an electronic printing system having programming means enabling a user to program instructions for print jobs; a source of image signals; memory means for storing said print jobs together with said image signals; and a printer for producing prints from said image signals in accordance with said instructions.

[0004] Such method and apparatus is known from L. J.FRAIM: "Secure Office Management System" published in proceedings of the Fall Joint Computer Conference, 1987, October 25-29, INFOMART; Dallas, Texas, pages 421-426.

[0005] In conventional light/lens copiers, document security has generally been grounded on physical possession of the document originals and the copies made while copier access and use has been based on billing considerations. In the case of document security, security for a user's originals and copies was attended to by the fact that the originals from which the copies were made as well as the copies themselves normally remained in the possession and control of the owner or in the hands of someone known to the owner and trusted to make copies. Control over copier access on the hand, if it existed at all, was generally based on assuring that the person using the copier and making copies was correctly billed or charged for the copies made. This for example led in the past to development and introduction of copy charge counters or meters which limited use of a copier to those persons having an account against which the cost of the copies could be charged. But generally, in the copier environment, little or no attention was given to security, and particularly to the security of the owner's files.

[0006] With the advent of electronic printing systems however, where the image is in the form of electrical signals or pixels, a user's electronic files, programs, etc., which may be confidential or personal in nature, are at least temporarily stored in the system. As a result, the owner's files may be available to anyone having access to the system for reading, copying, tampering, etc. A similar situation occurs with data that is transmitted to a communication channel to or from the system. Anyone having access to the system can intercept and gain access to the transmitted data for his own purposes.

[0007] In the prior art, security in the past has focused on computer systems as evidenced by U.S. Patent No. 4,713,753 to Boebert et al wherein there is disclosed a secure system architecture for a data processor in which a predefined security policy, stored in a secure processor, uses format control to prevent alteration of a program. U.S. Patents Nos. 4,525,780 to Bratt et al and 4,498,132 to Ahlstrom et al (which relies on U.S. Patent No. 4,525,780 for its description) disclose a data processing system having an addressing system for processing object based information with a protection scheme for controlling access rights to the information. And U.S. Patent No. 4,799,258 to Davies discloses a dual key system for controlling access to computers to assure a tamper resistant store.

[0008] Further in computer applications, a User Identification Code (UIC) technique has been used to control file access. In this technique, two numbers are provided per user, a group number and a member number. Each user accordingly is represented as a member of a group which may span a number of other users with a common need to share information. Further, each file has certain attributes associated with it, such as the UIC of the owner and the protection settings controlling READ and WRITE access. The UIC system however is limited in the levels of security that it can provide and has limited extensibility.

[0009] A second prior art technique of the type discussed in U.S. Patents Nos. 4,498,132 and 4,525,780 above is based upon access lists where each operation on a file is controlled by a list maintained by the file's owner of users who are granted or denied access. The list additionally may contain pre-defined group names and object enablements or restrictions. The disadvantages of this technique are the large amount of memory required and large amounts of processing overhead needed to maintain and verify the list.

[0010] In contrast, the present invention provides a security process for an electronic reprographic printer of the above mentioned type, which is characterized in that, in the step of giving said administrator power, user identification numbers are assigned at less secured sites and use of passwords by said users is enabled at more secure sites; in the step of providing user file security, the non-removable security label is assigned by said users; and in that said security process comprises the further steps: providing a site administrator; giving said site administrator control over user job programming options for said printer; isolating functions of said site administrator from user functions by assigning special identification number and password to said site administrator to prevent users from accessing said site administrator functions; and providing user file security by enabling users, to protect user files by user passwords, and to limit access of others to user files.

[0011] Further, the present invention provides an

electronic printing system of the above mentioned type characterized by system lockout means for controlling programming of print jobs on said system, said lockout means being responsive to input of a preset user identification number and user name to permit said user to program instructions for print jobs; first means to limit the source of said identification number to a preset identification number source for said system, said first means enabling said source to assign special identification numbers to users enabling identified users to program instructions for print jobs on said system; second means to allow at least some of said users to provide personal user passwords to limit access of others to a user's print jobs in said memory means; and third means to allow individual users to limit the ability of other users having access to said individual users' print jobs to change said print jobs following access.

[0012] In particular, the present invention provides a security process for an electronic reprographic printer, comprising the steps of: providing a security administrator; providing a security profile with discrete security levels for different classes of users under the control of the security administrator; giving the administrator power to assign user identification numbers at less secured sites, and enable use of passwords by the users at more secure sites; providing a site administrator; giving the site administrator control over user job programming options for the printer; isolating functions of the site administrator from user functions by assigning special identification number and password to the site administrator to prevent users from accessing the site administrator functions; and providing user file security by enabling users, to protect user files by user passwords, to limit access of others to user files, and to assign a non-removable security label to a user's files which prevents printing or displaying of the files without the security label.

IN THE DRAWINGS:

[0013]

Figure 1 is a view depicting an electronic printing system incorporating the security system of the present invention;
Figure 2 is a block diagram depicting the major elements of the printing system shown in Figure 1;
Figure 3 is a plan view illustrating the principal mechanical components of the printing system shown in Figure 1;
Figure 4 is a schematic view showing certain construction details of the document scanner for the printing system shown in Figure 1;
Figures 5A, 5B, and 5C comprise a schematic block diagram showing the major parts of the control section for the printing system shown in Figure 1;
Figure 6 is a block diagram of the Operating System, together with Printed Wiring Boards and shared line connections for the printing system shown in Figure 1;
Figure 7 is a view depicting an exemplary job programming ticket and job scorecard displayed on the User Interface (UI) touchscreen of the printing system shown in Figure 1;
Figure 8 is a view of the User Interface touchscreen on which is displayed a SECURITY card file having "Users", "Security Profile", and "Access Lists"icons, with the "Users" icon actuated to display a listing of users by name;
Figure 9 is a view in which a user is selected by highlighting and opening a SYSTEM ADMINISTRATOR window providing processing selections;
Figure 10 is a view displaying the User Profile for the user selected;
Figure 11 is a view displaying the "Privileges" card file for the user selected;
Figure 12 is a view showing the "Delete User?" options window opened;
Figure 13 is a view showing the " Assign New Owner" options window opened;
Figure 14 is a view showing the user "Profile Options" window opened to display the "New User Template" selections;
Figure 15 is a view of the User Interface touchscreen showing the "New User Template" following selection;
Figure 16 is a view showing the "Security Profile" card file for the site;
Figure 17 is a view showing the"Activity Log" for the site;
Figure 18 is a view showing the "Activity Log" in Figure 17 with the "Audit Trail Options" window opened;
Figure 19 is a view of the User Interface touchscreen depicting the "Access Lists" card file;
Figure 20 is a view showing the "Access Lists"card file of Figure 19 with a file window opened to display list selections:
Figure 21 is a view showing the "Access Lists"card file of Figure 19 with the "Delete List?" window opened;
Figure 22 is a view showing the "Member Name" file with names of members in a selected access list;
Figure 23 is a view showing the "Remove from list" selection window for removing members from the selected access list;
Figure 24 is a view showing the "Add Member" window for adding a member's name to the access list selected;
Figure 25 is a view showing the "Job Access Control" card enabling a file owner to set the access rights to the owner's files; and
Figure 26 is a plane view of a second embodiment in which the security system is externally administered.

[0014] Referring to Figures 1 and 2, there is shown an exemplary image printing system 2 for processing print jobs in accordance with the teachings of the present invention. Printing system 2 for purposes of explanation is divided into image input section 4, controller section 7, and printer section 8. In the example shown, image input section 4 has both remote and on-site image inputs, enabling system 2 to provide network,scan, and print services. Other system combinations may be envisioned such as a stand alone printing system with on-site image input (i.e., a scanner), controller, and printer; a network printing system with remote input, controller, and printer; etc. While a specific printing system is shown and described, the present invention may be used with other types of printing systems. For example, printer section 8 may instead use a different printer type such as ink jet, ionographic, etc.

[0015] Referring particularly to Figures 2-4, for off-site image input, image input section 4 has a network 5 with a suitable communication channel such as a telephone line enabling image data in the form of image signals or pixels from one or more remote sources to be input to system 2 for processing. Where the Page Description Language (PDL) of the incoming imaging data is different than the PDL used by system 2, suitable conversion means (not shown) are provided. Other remote sources of image data such as streaming tape, floppy disk, etc. may be envisioned.

[0016] For on-site image input, section 4 has a document scanner 6 with a transparent platen 20 on which documents 22 to be scanned are located. One or more linear arrays 24 are supported for reciprocating scanning movement below platen 20. Lens 26 and mirrors 28, 29, 30 cooperate to focus array 24 on a line like segment of platen 20 and the document being scanned thereon. Image data in the form of image signals or pixels from net 5 or array 24 are input to processor 25 for processing. After processing, the image signals are output to controller section 7.

[0017] Processor 25 converts the analog image signals output by array 24 to digital. Processor 25 further processes image signals as required to enable system 2 to store and handle the image data in the form required to carry out the job programmed. Processor 25 also provides enhancements and changes to the image signals such as filtering, thresholding, screening, cropping, scaling, etc.

[0018] Documents 22 to be scanned may be located on platen 20 for scanning by automatic document handler (ADF) 35 operable in either a Recirculating Document Handling (RDH) mode or a Semi-Automatic Document Handling (SADH) mode. A manual mode including a Book mode and a Computer Forms Feeder (CFF) mode are also provided, the latter to accommodate documents in the form of computer fanfold. For RDH mode operation, document handler 35 has a document tray 37 in which documents 22 are arranged in stacks or batches. The documents 22 in tray 37 are advanced by vacuum feed belt 40 and document feed rolls 41 and document feed belt 42 onto platen 20 where the document is scanned by array 24. Following scanning, the document is removed from platen 20 by belt 42 and returned to tray 37 by document feed rolls 44.

[0019] For operation in the SADH mode, a document entry slot 46 provides access to the document feed belt 42 between tray 37 and platen 20 through which individual documents may be inserted manually for transport to platen 20. Feed rolls 49 behind slot 46 form a nip for engaging and feeding the document to feed belt 42 and onto platen 20. Following scanning, the document is removed from platen 20 and discharged into catch tray 48.

[0020] For operation in the CFF mode, computer forms material is fed through slot 46 and advanced by feed rolls 49 to document feed belt 42 which in turn advances a page of the fanfold material into position on platen 20.

[0021] Referring to Figures 2 and 3, printer section 8 comprises a laser type printer and for purposes of explanation is separated into a Raster Output Scanner (ROS) section 87, Print Module Section 95, Paper Supply section 107, and Finisher 120. ROS 95 has a laser 91, the beam of which is split into two imaging beams 94. Each beam 94 is modulated in accordance with the content of an image signal input by acousto-optic modulator 92 to provide dual imaging beams 94. Beams 94 are scanned across a moving photoreceptor 98 of Print Module 95 by the mirrored facets of a rotating polygon 100 to expose two image lines on photoreceptor 98 with each scan and create the latent electrostatic images represented by the image signal input to modulator 92. Photoreceptor 98 is uniformly charged by corotrons 102 at a charging station preparatory to exposure by imaging beams 94. The latent electrostatic images are developed by developer 104 and transferred at transfer station 106 to a print media 108 delivered by Paper Supply section 107. Media 108 as will appear may comprise any of a variety of sheet sizes, types,and colors. For transfer, the print media is brought forward in timed registration with the developed image on photoreceptor 98 from either a main paper tray 110 or from auxiliary paper trays 112, or 114. The developed image transferred to the print media 108 is permanently fixed or fused by fuser 116 and the resulting prints discharged to either output tray 118, or to finisher 120. Finisher 120 includes a stitcher 122 for stitching or stapling the prints together to form books and a thermal binder 124 for adhesively binding the prints into books.

[0022] Referring to Figures 1, 2 and 5, controller section 7 is, for explanation purposes, divided into an image input controller 50, User Interface (UI) 52, system controller 54, main memory 56, image manipulation section 58, and image output controller 60.

[0023] The image data input from processor 25 of image input section 4 to controller section 7 is compressed by image compressor/ processor 51 of image input con-

troller 50 on PWB 70-3. As the image data passes through compressor/processor 51, it is segmented into slices N scanlines wide, each slice having a slice pointer. The compressed image data together with slice pointers and any related image descriptors providing image specific information (such as height and width of the document in pixels, the compression method used, pointers to the compressed image data, and pointers to the image slice pointers) are placed in an image file. The image files, which represent different print jobs, are temporarily stored in system memory 61 which comprises a Random Access Memory or RAM pending transfer to main memory 56 where the data is held pending use.

[0024] As best seen in Figure 1, UI 52 includes a combined operator controller/CRT display consisting of an interactive touchscreen 62, keyboard 64, and mouse 66. UI 52 interfaces the operator with printing system 2, enabling the operator to program print jobs and other instructions, to obtain system operating information, instructions, programming information, diagnostic information, etc. Items displayed on touchscreen 62 such as files and icons are actuated by either touching the displayed item on screen 62 with a finger or by using mouse 66 to point cursor 67 to the item selected and keying the mouse.

[0025] Main memory 56 has plural hard disks 90-1,90-2,90-3 for storing machine Operating System software, machine operating data, and the scanned image data currently being processed.

[0026] When the compressed image data in main memory 56 requires further processing, or is required for display on touchscreen 62 of UI 52, or is required by printer section 8, the data is accessed in main memory 56. Where further processing other than that provided by processor 25 is required, the data is transferred to image manipulation section 58 on PWB 70-6 where the additional processing steps such as collation, make ready, decomposition, etc are carried out. Following processing, the data may be returned to main memory 56, sent to UI 52 for display on touchscreen 62, or sent to image output controller 60.

[0027] Image data output to image output controller 60 is decompressed and readied for printing by image generating processors 86 of PWBs 70-7, 70-8 (seen in Figure 5A). Following this, the data is output by dispatch processors 88,89 on PWB 70-9 to printer section 8. Image data sent to printer section 8 for printing is normally purged from memory 56 to make room for new image data.

[0028] Referring particularly to Figures 5A-5C, control section 7 includes a plurality of Printed Wiring Boards (PWBs) 70, PWBs 70 being coupled with one another and with System Memory 61 by a pair of memory buses 72, 74. Memory controller 76 couples System Memory 61 with buses 72, 74. PWBs 70 include system processor PWB 70-1 having plural system processors 78; low speed I/O processor PWB 70-2 having UI communication controller 80 for transmitting data to and from UI 52; PWBs 70-3, 70-4, 70-5 having disk drive controller/processors 82 for transmitting data to and from disks 90-1, 90-2, 90-3 respectively of main memory 56 (image compressor/processor 51 for compressing the image data is on PWB 70-3); image manipulation PWB 70-6 with image manipulation processors of image manipulation section 58; image generation processor PWBs 70-7, 70-8 with image generation processors 86 for processing the image data for printing by printer section 8; dispatch processor PWB 70-9 having dispatch processors 88, 89 for controlling transmission of data to and from printer section 8; and boot control-arbitration-scheduler PWB 70-10.

[0029] Referring particularly to Figure 6, system control signals are distributed via a plurality of printed wiring boards (PWBs). These include EDN core PWB 130, Marking Imaging core PWB 132, Paper Handling core PWB 134, and Finisher Binder core PWB 136 together with various Input/Output (I/O) PWBs 138. A system bus 140 couples the core PWBs 130, 132, 134, 136 with each other and with controller section 7 while local buses 142 serve to couple the I/O PWBs 138 with each other and with their associated core PWB.

[0030] On machine power up, the Operating System software is loaded from memory 56 to EDN core PWB 130 and from there to the remaining core PWBs 132, 134, 136 via bus 140, each core PWB 130, 132, 134, 136 having a boot ROM 147 for controlling downloading of Operating System software to the PWB, fault detection, etc. Boot ROMs 147 also enable transmission of Operating System software and control data to and from PWBs 130, 132, 134, 136 via bus 140 and control data to and from I/O PWBs 138 via local buses 142. Additional ROM, RAM, and NVM memory types are resident at various locations within system 2.

[0031] Referring to Figure 7, jobs are programmed in a Job Program mode in which there is displayed on touchscreen 62 a Job Ticket 150 and a Job Scorecard 152 for the job being programmed. Job Ticket 150 displays various job selections programmed while Job Scorecard 152 displays the basic instructions to the system for printing the job.

[0032] To control access to printing system 2 at a site and protect any sensitive data and files stored in the system memory, the security system of the present invention is provided. When invoked, a user in order to gain access to printing system 2 must authenticate himself by a special User Identification number (User ID). Where a password option is enabled, the user is also required to enter his password. As will appear, a Security administrator assigns the User ID while the user creates his own password when allowed to do so.

[0033] The site, which is the business location for the printing system 2, has the ability to define the level of security desired. Generally, the levels of security are:

(1) no security except for administrative functions controlled by either a site administrator or a security

administrator. These administrative functions are the type which require access controls to protect sensitive information and performance variables for the system. At this security level, no user would be required to log onto printing system and each user would have full access to any function available on the system

(2) a partially secure site would allow User IDs to be assigned to some users at the Security Administrator's discretion. This would give these users access to certain privileged system functions.

(3) a fully secured site where all users are assigned a User ID by the Security administrator.

(4) fully secured site with passwords would allow some or all users, at the discretion of the Security administrator, to employ their own password to control access to the user's own files that are in the system.

[0034] A Site administrator is normally provided (although one administrator may serve in both Site and Security Administrator capacities). The Site administrator is considered a privileged user and as such has certain privileges over and above those of either a secure or non-secure user. The Site administrator typically establishes the programming features and functions that the site will have, the system default settings, etc., and has shared operating functions such as billing, accounting, etc.

[0035] A Security administrator is a trusted individual charged with the responsibility for creating and implementing the security rules of printing system 2 consistent with the security level desired by the site. In this capacity, the Security administrator controls access to the programming features, administration, and service of printing system 2. Programming functions and features comprise the different level of system job programming choices that are made available to a user by the Site administrator. Security administration relates to the process by which security at the site is administered while service refers to the security that governs access by service or repair personnel (referred to herein as Tech Reps.).

[0036] To enable the Security administrator to carry out his duties, the Security administrator establishes and maintains a User Profile for each user. The User Profile allows the Security administrator to establish a security profile for each user to whom the Security administrator assigns a User ID plus other security enablements such as user passwords, rights to access different system programming functions, etc. depending upon the security level of the site. As will be understood, access to the user profile is limited to whatever rights the Security administrator has.

[0037] Referring to Figures 8-12, on entering the "Administration" mode, there is displayed on touchscreen 62 certain card files including a "SECURITY" card file 200 on which are displayed "Users", "Security Profile", and "Access Lists" icons 201, 202, 203 respectively. Actuation of "Users" icon 201 causes a "User Name" file 205 to be displayed listing the names of all users at the site to whom a User ID has been assigned, the user's ID, and whether the user is "Active" or "Inactive". Up and down scrolling icons 207, 208 permit scrolling of file 205 to allow reading of all the user names.

[0038] Where the Security administrator desires to view the User Profile for a particular user, a "Users"icon 210 in "Users Name" file 205 is actuated to display a "SYSTEM ADMINISTRATION" window 212 having "Open Profile", "Activate", "Delete", and "Close" selections. Moving window 212 so that the window pointer 212' is opposite the name of the user whose User Profile is to be viewed and actuating "Open Profile"displays the User Profile 215 for the user name selected. As shown in Figure 10, User Profile 215 identifies the "User Status", "User Name", "User ID", whether the user has a password or not, and the user's "Default Account". Additionally, a "Job Access Control" icon 217 and a "Privileges" icon 219 are displayed.

[0039] Selecting "Privileges" 219 displays the privileges granted to the user as shown in Figure 11. These consist of"Administration", "Service", and "Feature Access".

[0040] The Security administrator ordinarily has "Administration" privileges for "Security" while the Site administrator has privileges for "Site". A single person may have privileges for "Both". Special ID numbers prevent users from gaining access to the security and administration functions performed by the administrator or administrators.

[0041] Referring to Figures 9,12, and 13, actuating "Delete" in window 212 displays a "Delete User?" window 221 with "Yes" and "No" options. Actuation of "Yes" deletes the current user and displays an "Assign New Owner" window 223 through which the Security administrator can assign a new owner for the former user's jobs currently in the system if desired. For this, and referring to Figures 14-15, a "Profile Options" window 225 is opened displaying a "New User Template" selection 226. Actuation of the "New User Template" 226 displays the template 228 seen in Figure 15 by which a User Profile 215 for the new user is created.

[0042] A similar procedure is followed where a "New User" is to be added to the users given access to printing system 2. In that case, the "New User"icon 230 in "Users Name" file 205 (Figure 8) is actuated.

[0043] The Security administrator may also be given the ability to set up certain user independent functions such as the number of attempts a user can make to logon before lockout, minimum User ID length, minimum password length, etc. depending on the security level of the site. For this, and referring to Figures 8 and 16, the Security Profile icon 202 is actuated to display "Security Profile" scorecard 232 showing the current security setup of the site. These include whether or not user logon is required ("Logon Required"), the minimum number of

characters in the user's ID ("Minimum User ID Length"), the length of a sessions ("Session Timeout"), the maximum number of logon attempts by a user that are allowed ("Maximum Failed Logons"), if a password is required ("Password required for"), the "Minimum Password Length", "Password History Length", and "Password Expiration".

[0044] An "Activity Log" icon 235 enables the Security administrator to access data when auditing security relevant functions and to activate auditing functions which will monitor and log system data, user logon/off, access to secure items, power on/off, etc. Actuating icon 235 displays an "Activity Log" scorecard 237 (Figure 17) with a series of system auditing options for monitoring the number of times certain activities such as "Logon/Logoff", etc. take place. The site security enablements such as "Security Configuration" are also displayed for selection together with an option to print out a hard copy of the activity log ("Print Activity Log") and to reset the log ("Reinitialize Activity Log") as shown in Figure 18.

[0045] Referring to Figures 8 and 19-24, the Security administrator may also set up access lists grouping users who have security access to a common file. Actuating "Access List" icon 203 displays a card file 239 of names for a specific job with a selection window 240. As in the case of individual users discussed previously, the Security administrator may select a list for deletion (Figure 21), or open a list to display the members names (Figure 22), or remove individual members from the list (Figure 23), or add new members to the list (Figure 24).

[0046] As will be understood, the set of operations and program selections which an user is allowed to perform on a particular job or directory object is a direct consequence of the user's clearance. Control over access to jobs and data stored in printing system 2 originates with the data creator or owner and governs the operations which a user is allowed to perform on files resident in the system.

[0047] Referring to Figures 10 and 25, actuation of "Job Access Control" icon 217 displays a "Job Access Control" scorecard 241 allowing a user to impose security restrictions on the user's files or jobs that are resident in printing system 2. The security limitations fall into two general classes: "COPIED and MODIFIED" and "COPIED" only. Each class is subdivided into: "All Users" 242, "Job Owner" 244, "Access List" 246, and "None" 248. "All Users" allows anyone to modify and/or copy the user's jobs, "Job Owner" allows only the job owner to modify and/or copy the user's jobs, "Access List" lists the names of users who are allowed to modify and/or copy the user's jobs, and "None" prevents anyone, including the job owner, from modifying and/or copying the user's jobs.

[0048] Tech Reps have their own security protection in the form of a Tech Rep ID number which is assigned either when printing system 2 is manufactured or when system 2 is installed. The Tech Rep ID number can be used to control down to the work support group level or any other service control level desired.

[0049] Once the Tech Rep ID number is assigned, the service organization to which the Tech Rep belongs can assign a password to protect both the service organization and the site by limiting access to only Tech Reps who have the correct password. The Tech Rep password can be changed at any time by the service organization. Further the service organization can assign special Tech Rep passwords to each site to further enhance site and/or the service organization security requirements.

[0050] Additionally, the service organization can also assign advanced levels of servicing access to selected personnel at individual sites. Typically this would be to site personal who have attended special training courses enabling them to perform more difficult and complex service operations on printing system 2 than the typical user would be able to do. The Site administrator normally would decide the site personal to be selected for this purpose with the Security administrator controlling special service access rights through "Service" selection under "PRIVILEGE" as shown in Figure 11.

[0051] While files are protected through the password mechanism and/or by the ability of a user to decide the appropriate access rights of others to the user's files as described, the operator also has the ability to assign a security label to a file. To enable the use of security labels, the system described and claimed in copending application SN 07/590633, filed on Sept. 28, 1990 (corresponding to EP-A-0 478 335), entitled "Process For Merging Logos With Prints Produced By Electronic Printing Machines" in the names of Hengst et al (Attorney Docket No. D/89288) may be used for this purpose. A folder for security labels is stored in the system Merge Library into which the operator places his security label (s). In doing so, the user can identify the location of the security label on the page and the page side on which the security label is to appear. Printing system 2 assures that once selected, the user's file will never be displayed on touchscreen 62 or printed by printer section 8 without the security label selected by the user being present. In addition, printing system 2 provides the operator with the option of placing the security label in the background of the image displayed on touchscreen 62 or printed by printer section 8. This prevents anyone from removing the label since the security label will appear associated directly with the image itself.

[0052] In addition to security labels, printing system 2 provides the capability of printing other label types such as labels with an automatic date-time stamp along the edge or edges of the image displayed or printed,a label identifying the site of the printing system making the prints, a label identifying the image owner, etc.

[0053] Referring to Figure 26, while a security system internal to a printing system 2 has been shown and described, control over the security of one or more sites may be established from a remote site, referred to herein as security center 300. Center 300 is coupled to the

printing system site or sites by a communication channel 305 such as a telephone wire. An external data base or memory 308 at security center 300 serves as a storage medium for the users' User Profiles 215 and ID numbers following establishment by the Security administrator. The users individual passwords are stored in the internal data base or memory 56 of the printing system that is used by the user.

[0054] In order to gain access to one or more of the printing systems 2, the user enters his user ID number and password using keyboard 64. The user ID number is transmitted via channel 305 to the external data base 308 where a comparison is made with the user ID numbers held in data base 308. Where the user ID number entered at the site by the user matches a number held in data base 308, an authentication signal is sent via channel 305 to the printing system controller section 7, authenticating the user. Concurrently, the password entered by the user is compared with passwords held in the system internal data base and where a match is found, a second authentication signal is generated and sent to controller section 7 of the printing system. On receipt of user authentication, controller section 7 enables the user to access the printing system.

Claims

1. Security process for an electronic reprographic printer, comprising the steps of:

   a) providing a security administrator;

   b) providing a security profile with discrete security levels for different classes of users under the control of said security administrator;

   c) giving said administrator power to

      1) assign user identification numbers, and

      2) enable use of passwords by said users;

   d) providing user file security by assigning a non-removable security label to a user's files which prevents printing or displaying of said files without said security label;
   characterized in that

      in step c), user identification numbers are assigned at less secured sites and use of passwords by said users is enabled at more secure sites;

      in step d), the non-removable security label is assigned by said users;

   and in that said security process comprises the further steps:

   e) providing a site administrator;

   f) giving said site administrator control over user job programming options for said printer;

   g) isolating functions of said site administrator from user functions by assigning special identification number and password to said site administrator to prevent users from accessing said site administrator functions; and

   h) providing user file security by enabling users,

      1) to protect user files by user passwords, and

      2) to limit access of others to user files.

2. The process according to claim 1 including the step of:

   providing user file security by limiting user access to printer programming features.

3. The process according to claim 1 including the step of:

   providing user file security by restricting user access to printer programming features that allow only moving or changing of files.

4. The process according to claim 1 including the step of:

   restricting access to complex printer programming features to avoid printer downtime.

5. The process according to claim 1 including the step of:

   restricting user access to pre-selected printer programming features to reduce personal use of printer.

6. An electronic printing system having programming means enabling a user to program instructions for print jobs; a source of image signals; memory means for storing said print jobs together with said image signals; and a printer for producing prints from said image signals in accordance with said instructions,
   characterized by

   a) system lockout means for controlling programming of print jobs on said system, said lockout means being responsive to input of a

preset user identification number and user name to permit said user to program instructions for print jobs;

b) first means to limit the source of said identification number to a preset identification number source for said system, said first means enabling said source to assign special identification numbers to users enabling identified users to program instructions for print jobs on said system;

c) second means to allow at least some of said users to provide personal user passwords to limit access of others to a user's print jobs in said memory means; and

d) third means to allow individual users to limit the ability of other users having access to said individual users' print jobs to change said print jobs following access.

Patentansprüche

1. Verfahren zum Schaffen von Sicherheit für eine elektronische reprografische Druckvorrichtung, umfassend die Schritte:

   a) zur Verfügung stellen eines Sicherheitsadministrators;

   b) zur Verfügung stellen eines Sicherheitsprofils mit diskreten Sicherheitsniveaus für verschiedene Klassen von Benutzern unter der Verwaltung des Sicherheitsadministrators;

   c) Ausstatten des Administrators mit der Ermächtigung

      1) Benutzeridentifikationsnummern zuzuweisen, und

      2) den Benutzern eine Verwendung von Paßwörtern zu ermöglichen;

   d) zur Verfügung stellen eines Benutzerdateischutzes durch Zuweisen einer nichtentfernbaren Schutzmarkierung zu Dateien eines Benutzers, was ein Drucken oder Anzeigen der Dateien ohne Schutzmarkierung verhindert; **dadurch gekennzeichnet,** daß

      in Schritt c) Benutzeridentifikationsnummern an weniger gesicherten Standorten zugewiesen werden und die Verwendung der Paßwörter durch die Benutzer an sichereren Orten ermöglicht wird;

      in Schritt d) die nichtentfernbare Schutzmarkierung durch die Benutzer zugewiesen wird;

   und daß das Verfahren zum Schaffen von Sicherheit die weiteren Schritte aufweist:

   e) zur Verfügung stellen eines Standortadministrators;

   f) Zuweisen der Verwaltung von Benutzerjobprogrammieroptionen für die Druckvorrichtung an den Standortadministrator;

   g) Isolieren von Funktionen des Standortadministrators von Benutzerfunktionen durch Zuweisen spezieller Identifikationsnummern und Paßwörter an den Standortadministrator, so daß verhindert wird, daß Benutzer auf die Standortadministratorfunktionen zugreifen; und

   h) zur Verfügung stellen eines Benutzerdateischutzes, dadurch daß den Benutzern ermöglicht wird,

      1) Benutzerdateien durch Paßwörter zu schützen, und

      2) den Zugriff von anderen auf die Benutzerdateien einzuschränken.

2. Das Verfahren nach Anspruch 1, umfassend den Schritt:

   zur Verfügung stellen eines Benutzerdateischutzes durch Einschränken des Benutzerzugriffs auf die Druckvorrichtungsprogrammiermerkmale.

3. Das Verfahren nach Anspruch 1, umfassend den Schritt:

   zur Verfügung stellen eines Benutzerdateischutzes durch Beschränken des Benutzerzugriffs auf Druckvorrichtungsprogrammiermerkmale, die ein Verschieben oder Ändern von Dateien ermöglichen.

4. Das Verfahren nach Anspruch 1, umfassend den Schritt:

   Beschränken des Zugriffs auf komplexe Druckvorrichtungsprogrammiermerkmale, um eine Stillstandzeit der Druckvorrichtung zu vermeiden.

5. Das Verfahren nach Anspruch 1, umfassend den

Schritt:

Beschränken des Benutzerzugriffs auf vorausgewählte Druckvorrichtungsprogrammiermerkmale, um den persönlichen Gebrauch der Druckvorrichtung zu verringern.

6. Ein elektronisches Drucksystem mit einer Programmiereinrichtung, die einem Benutzer ermöglicht, Anweisungen für Druckjobs zu programmieren; eine Bildsignalquelle; eine Speichereinrichtung zum Speichern der Druckjobs zusammen mit den Bildsignalen; und eine Druckvorrichtung zum Erstellen von Druckerzeugnissen aus den Bildsignalen gemäß den Anweisungen,
gekennzeichnet durch

a) eine Systemsperreinrichtung zum Steuern der Programmierung von Druckjobs auf dem System, wobei die Sperreinrichtung auf Eingabe einer voreingestellten Benutzeridentifikationsnummer und eines Benutzernamens so anspricht, daß dem Benutzer ermöglicht wird, die Anweisungen für Druckjobs zu programmieren;

b) eine erste Einrichtung zum Einschränken der Quelle der Identifikationsnummer auf eine vorbestimmte Identifikationsnummernquelle für das System, wobei die erste Einrichtung der Quelle ermöglicht, spezielle Identifikationsnummern an Benutzer zuzuweisen, wobei identifizierten Benutzern ermöglicht wird, die Anweisungen für Druckjobs auf dem System zu programmieren;

c) eine zweite Einrichtung, die es wenigstens einigen der Benutzer ermöglicht, persönliche Benutzerpaßwörter zu vergeben, um den Zugriff anderer auf Druckjobs eines Benutzers in der Speichereinrichtung einzuschränken; und

d) eine dritte Einrichtung, die es individuellen Benutzern ermöglicht, die Möglichkeit anderer Benutzer, auf die Druckjobs der individuellen Benutzer zur Änderung der Druckjobs nach dem Zugriff, einzuschränken.

Revendications

1. Procédé de sécurité pour une imprimante reprographique électronique, comprenant les étapes consistant à :

a) fournir un administrateur de sécurité ;

b) fournir un profil de sécurité comportant des niveaux de sécurité discrets pour différentes classes d'utilisateurs sous la commande dudit administrateur de sécurité ;

c) donner audit administrateur le pouvoir de

1) affecter des numéros d'identifications utilisateur, et
2) permettre l'utilisation de mots de passe par lesdits utilisateurs ;

d) procurer la sécurité du fichier utilisateur en affectant une étiquette de sécurité non enlevable au fichier utilisateur qui empêche l'impression ou l'affichage desdits fichiers sans ladite étiquette de sécurité ;
caractérisé en ce que

à l'étape c), les numéros d'identification d'utilisateur sont affectés à des sites moins sûr et l'utilisation des mots de passe par lesdits utilisateurs est activée à des sites plus sûrs ;
dans l'étape d), l'étiquette de sécurité non enlevable est affectée par lesdits utilisateurs ;
et en ce que ledit procédé de sécurité comprend les étapes supplémentaires consistant à :

e) fournir un administrateur de site ;

f) donner audit administrateur de site la commande sur les options de programmation de travaux pour ladite imprimante ;

g) isoler les fonctions dudit administrateur de site des fonctions de l'utilisateur en affectant un numéro d'identification spécial et un mot de passe spécial audit administrateur de site pour empêcher les utilisateurs d'accéder auxdites fonctions d'administrateur de site ; et

h) procurer une sécurité de fichier utilisateur en permettant aux utilisateurs,

1) de protéger les fichiers utilisateur par des mots de passe utilisateur, et
2) de limiter l'accès des autres personnes au fichier d'utilisateur.

2. Procédé selon la revendication 1, incluant l'étape consistant à :

procurer une sécurité de fichiers utilisateur en limitant l'accès par les utilisateurs aux options de programmation de l'imprimante.

3. Procédé selon la revendication 1, incluant l'étape

consistant à :

procurer une sécurité des fichiers utilisateur en limitant l'accès par les utilisateurs aux options de programmation d'imprimante qui permettent seulement le déplacement ou le changement des fichiers.

4. Procédé selon la revendication 1, incluant l'étape consistant à :

limiter l'accès aux options de programmation d'imprimante complexe pour éviter les temps d'arrêt de l'imprimante ;

5. Procédé selon la revendication 1, incluant l'étape consistant à :

limiter l'accès aux utilisateurs à des options de programmation d'imprimante présélectionnées pour réduire l'utilisation personnelle de l'imprimante.

6. Système d'impression électronique comportant un moyen de programmation permettant à un utilisateur de programmer des instructions pour des travaux impression ; une source de signaux d'image ; un moyen de mémoire pour mémoriser lesdits travaux impression en même temps que lesdits signaux d'image ; et une imprimante pour produire les impressions à partir desdits signaux d'image en conformité avec lesdites instructions,
caractérisé par

a) un moyen d'attribution exclusive de ressources du système pour commander la programmation des travaux impression ledit système, ledit moyen d'attribution exclusive de ressource étant sensible à une entrée d'un numéro d'identification d'utilisateur préétabli et d'un nom d'utilisateur pour permettre audit utilisateur de programmer des instructions pour les travaux à imprimer ;
b) un premier moyen pour limiter la source dudit numéro d'identification à une source de numéro d'identification préétabli pour ledit système, ledit premier moyen permettant à ladite source d'affecter des numéros d'identification spéciaux aux utilisateurs permettant aux utilisateurs identifiés de programmer des instructions pour les travaux d'impression sur ledit système ;
c) un second moyen pour permettre au moins à certains desdits utilisateurs de délivrer des mots de passe d'utilisateur personnels pour limiter l'accès des autres aux travaux d'impression de l'utilisateur dans ledit moyen de mémoire ; et
d) un troisième moyen pour permettre aux utilisateurs individuels de limiter l'aptitude des autres utilisateurs, comportant l'accès auxdits travaux d'impression d'utilisateur individuel de changer lesdits accés aux travaux d'impression suivants.

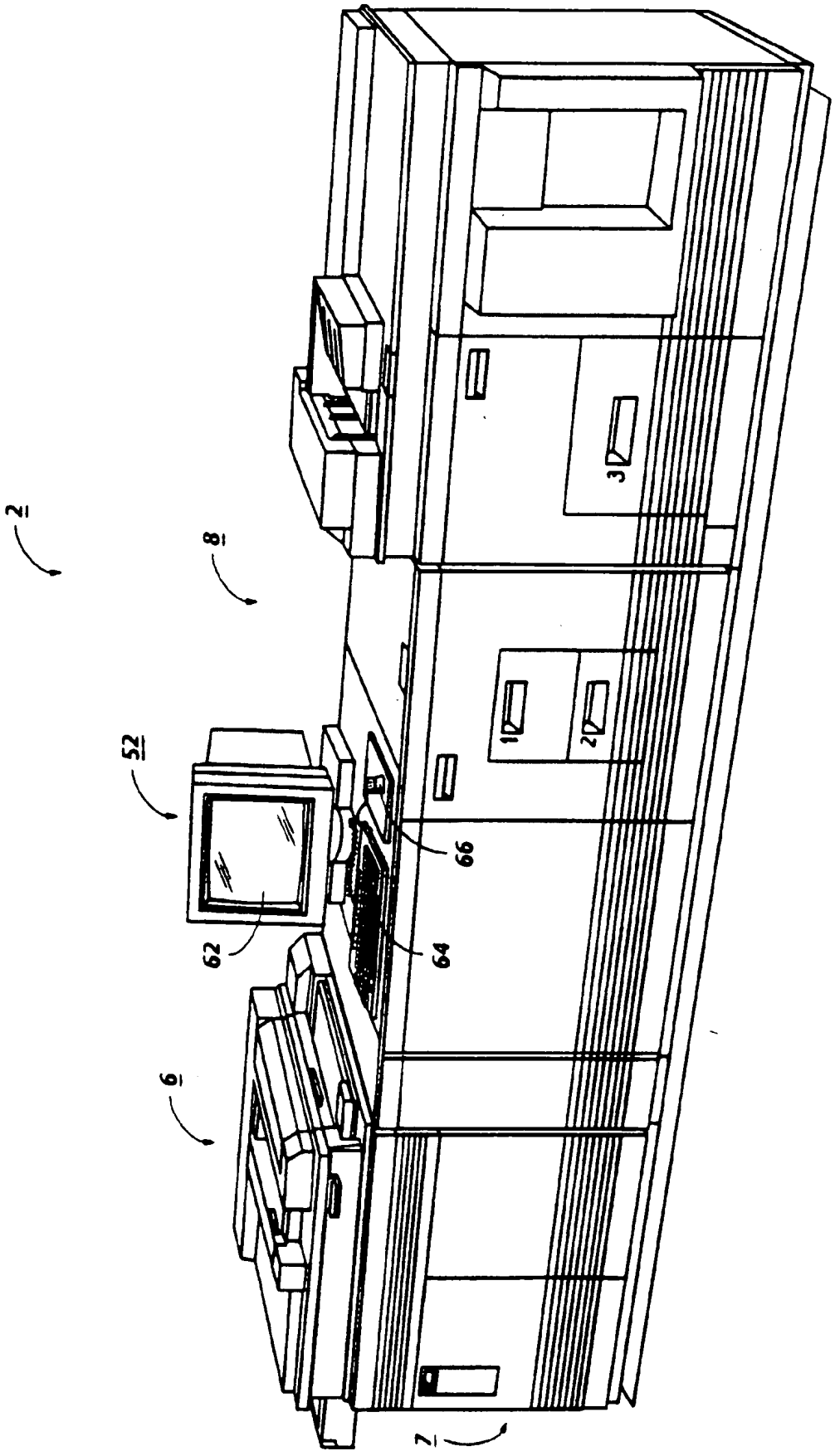


FIG. 1

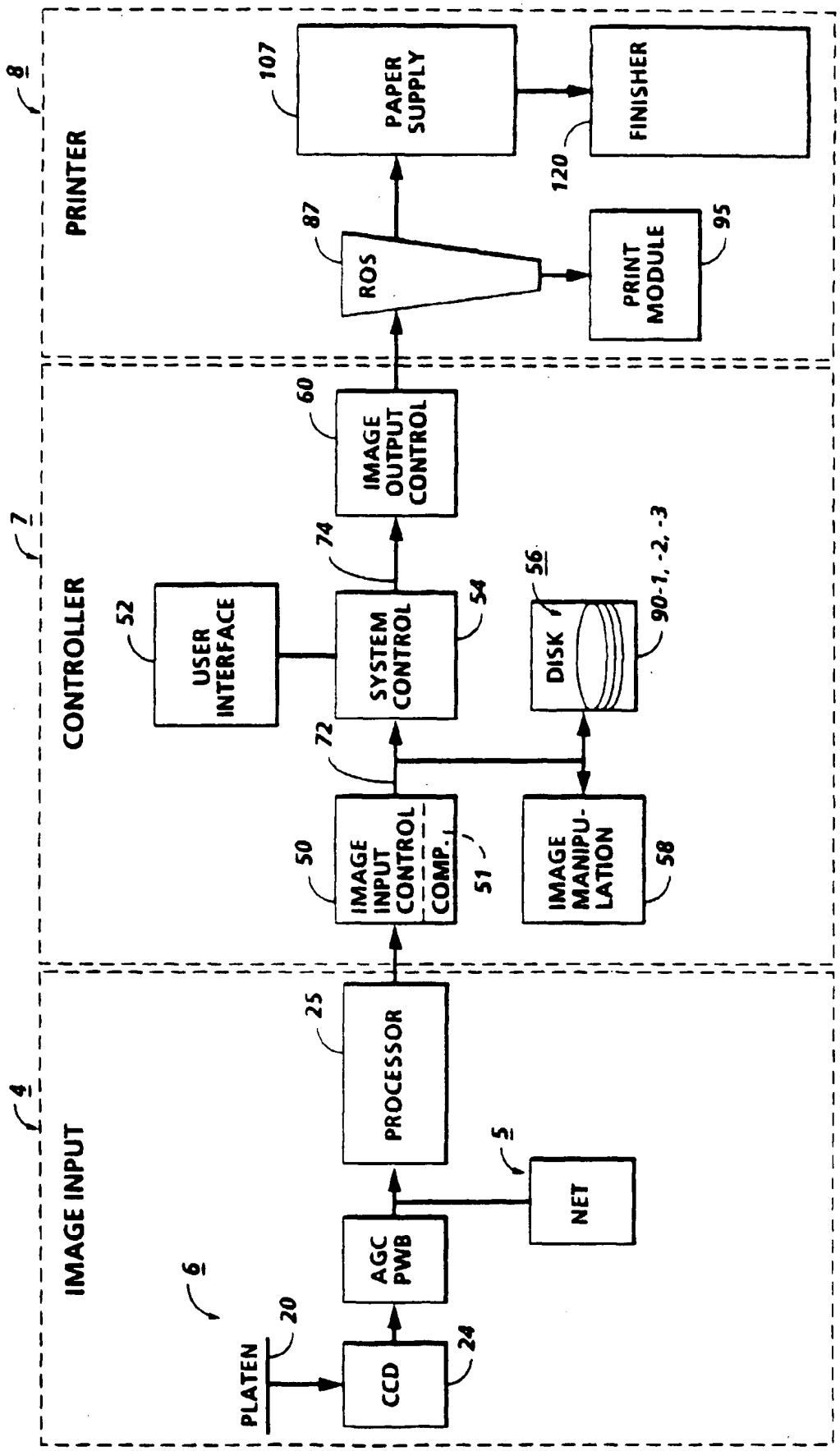

8
PRINTER
107
PAPER SUPPLY
FINISHER
120
87
ROS
PRINT MODULE
95
7
CONTROLLER
60
IMAGE OUTPUT CONTROL
74
52
USER INTERFACE
SYSTEM CONTROL
54
56
DISK
90-1, -2, -3
72
50
IMAGE INPUT CONTROL
COMP.
51
IMAGE MANIPU-LATION
58
4
IMAGE INPUT
25
PROCESSOR
5
NET
6
AGC PWB
PLATEN
20
CCD
24

FIG. 2

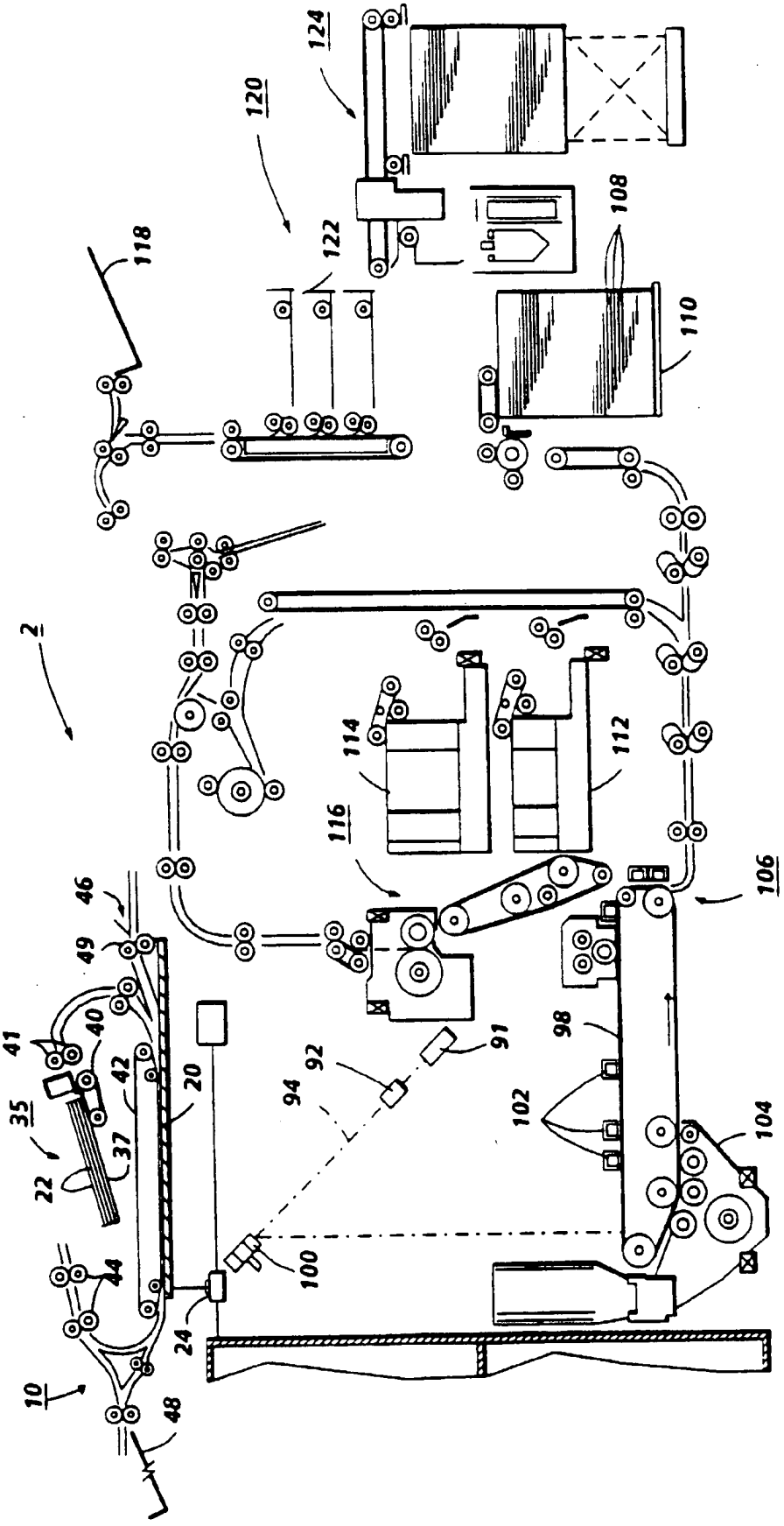

124
120
118
122
108
110
2
114
112
116
106
46
49
40
41
42
20
35
37
22
44
24
10
48
91
92
94
98
102
104
100

FIG. 3

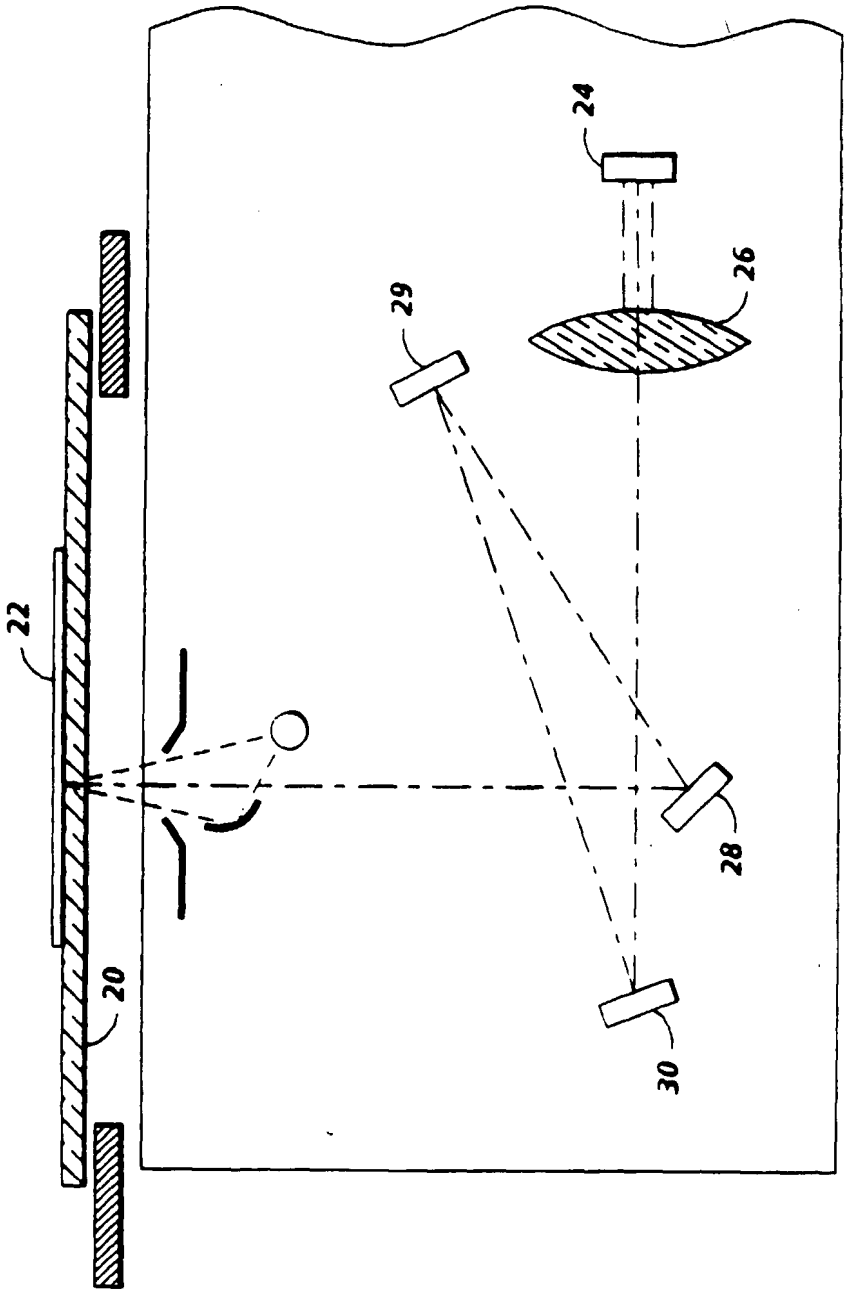


FIG. 4

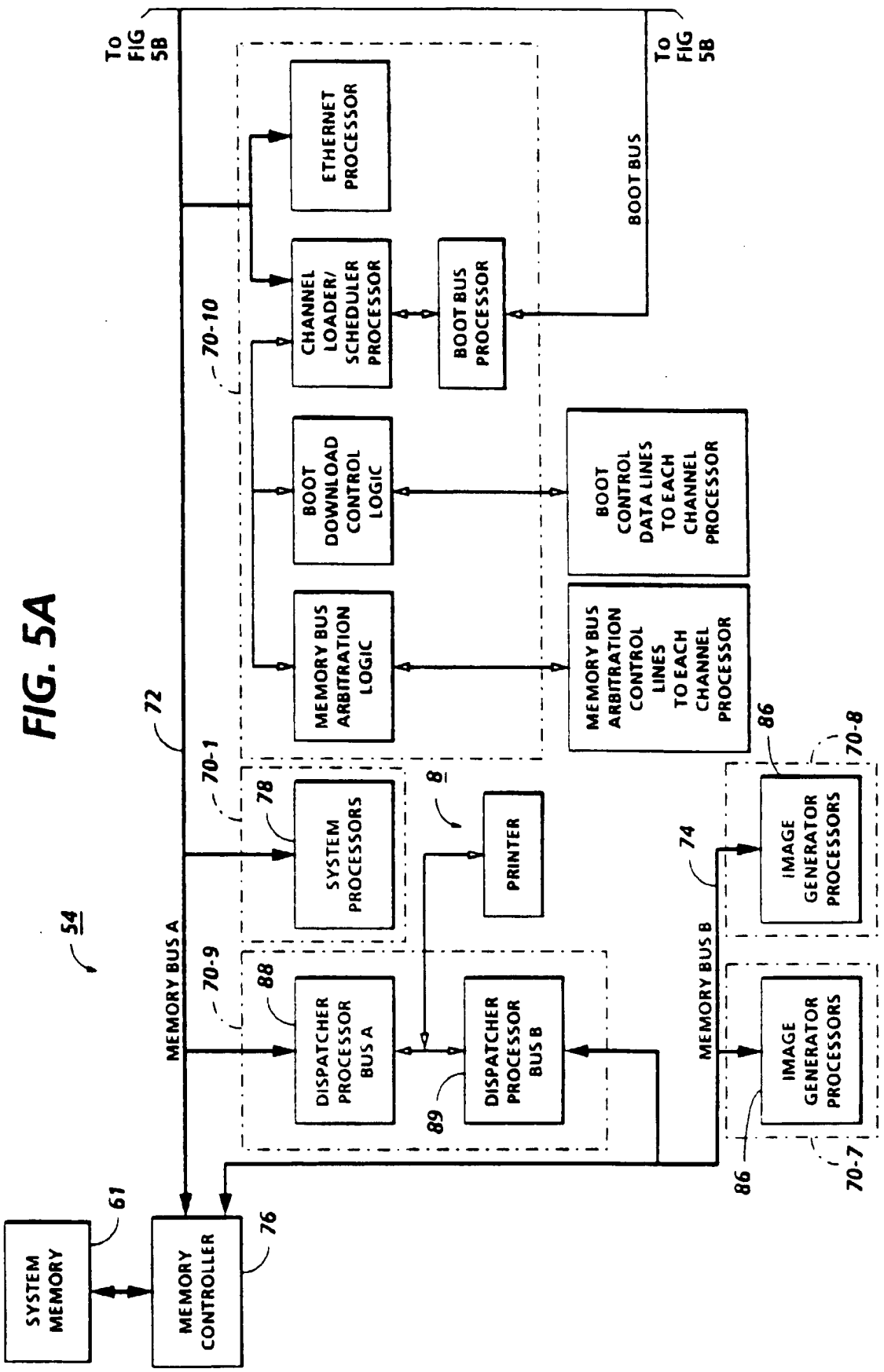

To FIG 5B
To FIG 5B
ETHERNET PROCESSOR
CHANNEL LOADER/ SCHEDULER PROCESSOR
BOOT BUS PROCESSOR
BOOT BUS
70-10
BOOT DOWNLOAD CONTROL LOGIC
BOOT CONTROL DATA LINES TO EACH CHANNEL PROCESSOR
MEMORY BUS ARBITRATION LOGIC
MEMORY BUS ARBITRATION CONTROL LINES TO EACH CHANNEL PROCESSOR
72
70-1
78
SYSTEM PROCESSORS
8
PRINTER
54
MEMORY BUS A
70-9
88
DISPATCHER PROCESSOR BUS A
DISPATCHER PROCESSOR BUS B
89
74
MEMORY BUS B
86
70-8
IMAGE GENERATOR PROCESSORS
IMAGE GENERATOR PROCESSORS
86
70-7
SYSTEM MEMORY
61
MEMORY CONTROLLER
76

FIG. 5A

FIG. 5B

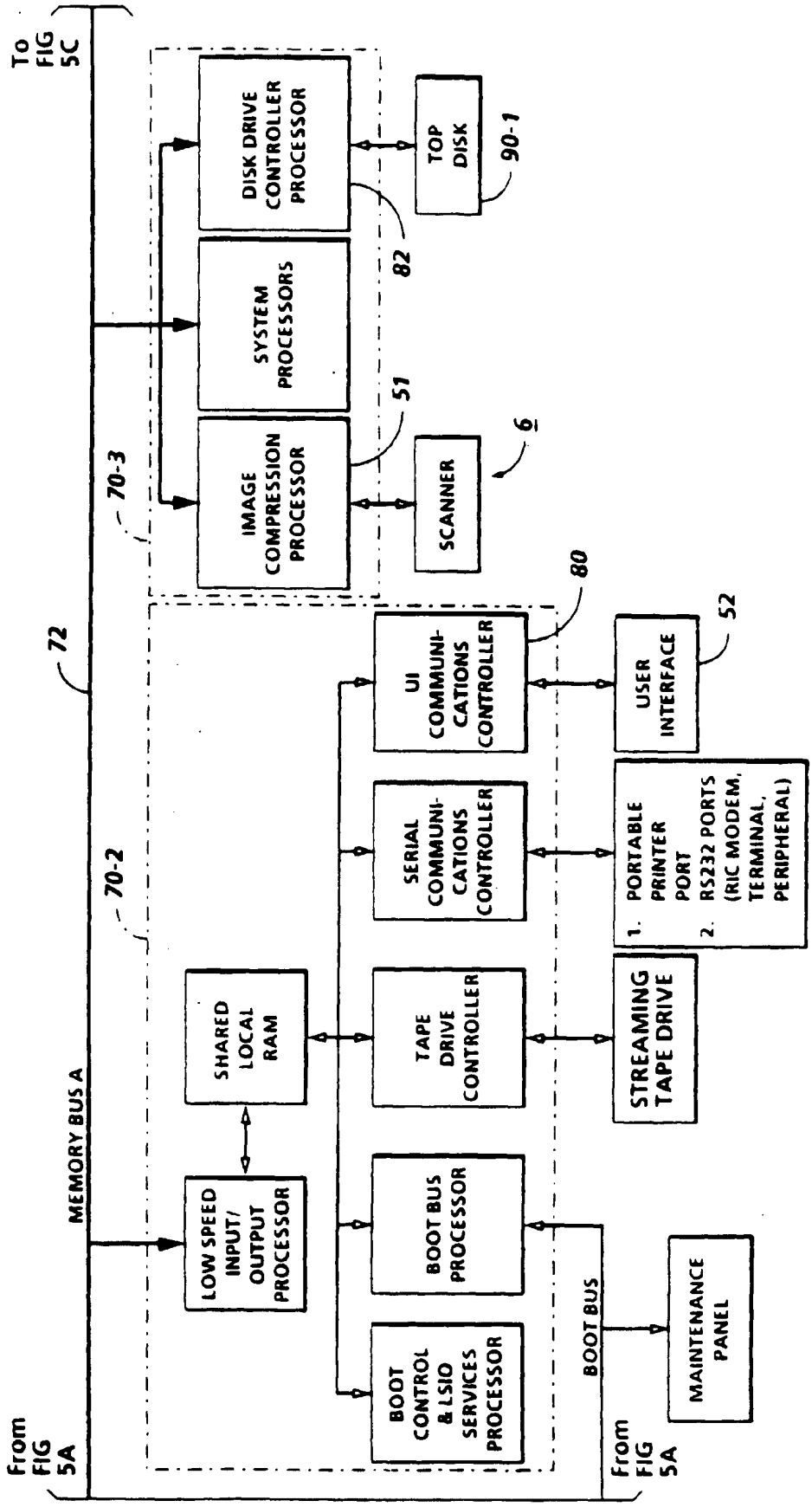
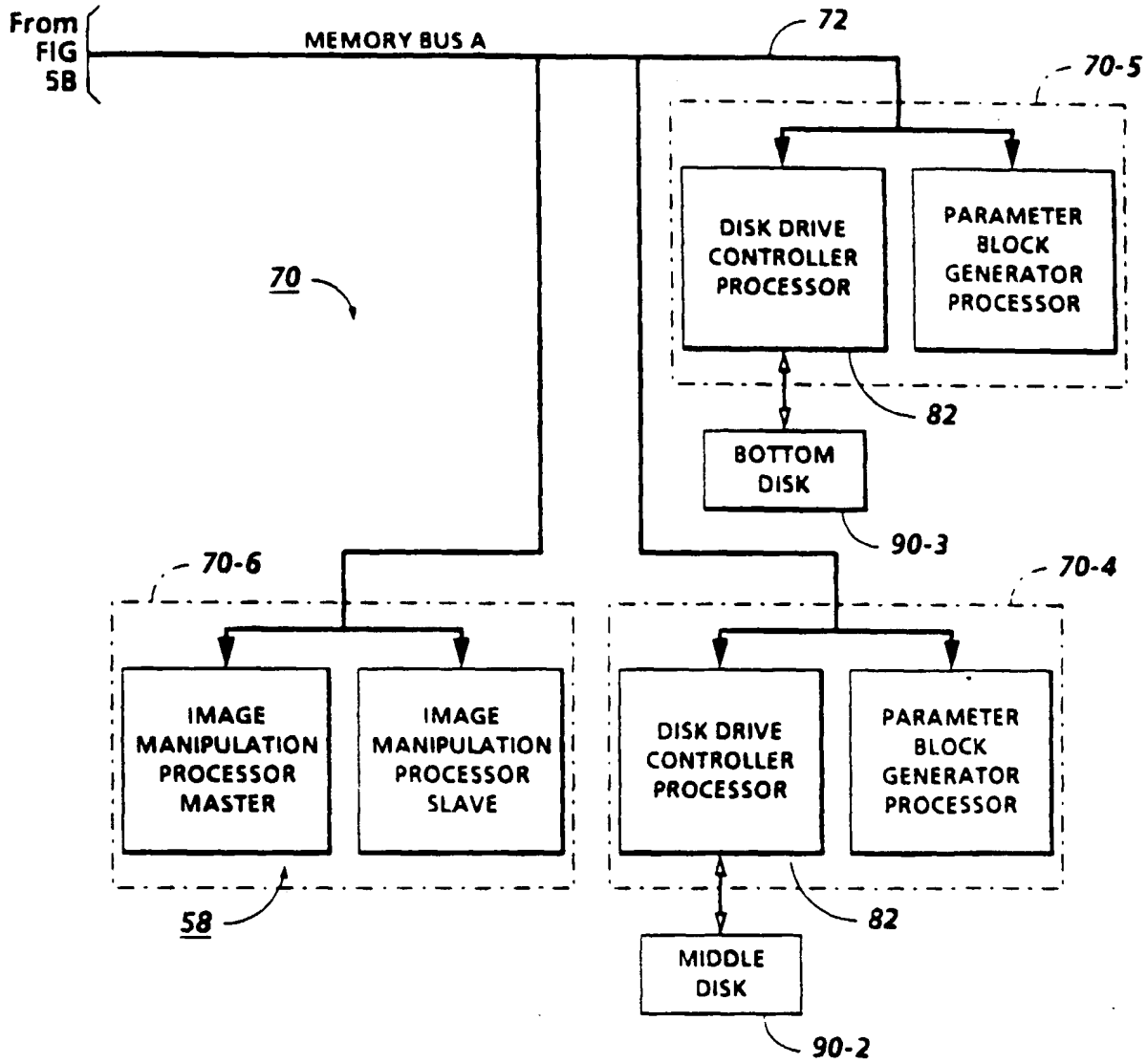

To FIG 5C
DISK DRIVE CONTROLLER PROCESSOR
TOP DISK
90-1
82
SYSTEM PROCESSORS
IMAGE COMPRESSION PROCESSOR
51
SCANNER
6
70-3
72
80
UI COMMUNI-CATIONS CONTROLLER
USER INTERFACE
52
70-2
SERIAL COMMUNI-CATIONS CONTROLLER
1. PORTABLE PRINTER PORT
2. RS232 PORTS (RIC MODEM, TERMINAL, PERIPHERAL)
SHARED LOCAL RAM
TAPE DRIVE CONTROLLER
STREAMING TAPE DRIVE
MEMORY BUS A
LOW SPEED INPUT/ OUTPUT PROCESSOR
BOOT BUS PROCESSOR
BOOT CONTROL & LSIO SERVICES PROCESSOR
BOOT BUS
MAINTENANCE PANEL
From FIG 5A
From FIG 5A

FIG. 5C


From FIG 5B
MEMORY BUS A
72
70-5
DISK DRIVE CONTROLLER PROCESSOR
PARAMETER BLOCK GENERATOR PROCESSOR
70
82
BOTTOM DISK
90-3
70-6
70-4
IMAGE MANIPULATION PROCESSOR MASTER
IMAGE MANIPULATION PROCESSOR SLAVE
DISK DRIVE CONTROLLER PROCESSOR
PARAMETER BLOCK GENERATOR PROCESSOR
58
82
MIDDLE DISK
90-2

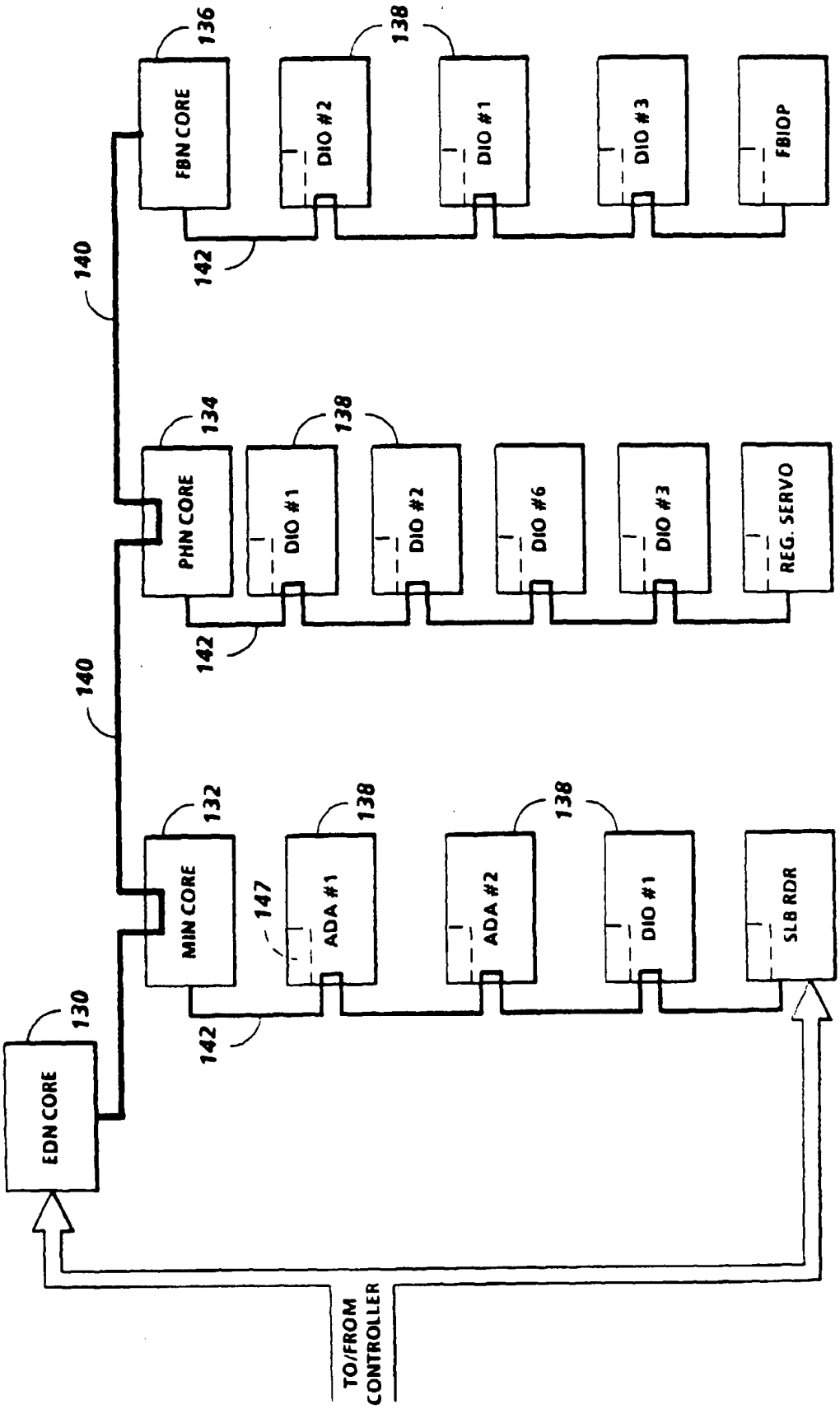

EDN CORE
130
MIN CORE
132
PHN CORE
134
FBN CORE
136
DIO #2
DIO #1
DIO #3
FBIOP
ADA #1
ADA #2
DIO #1
SLB RDR
DIO #1
DIO #2
DIO #6
DIO #3
REG. SERVO
138
140
142
147
TO/FROM CONTROLLER

FIG. 6

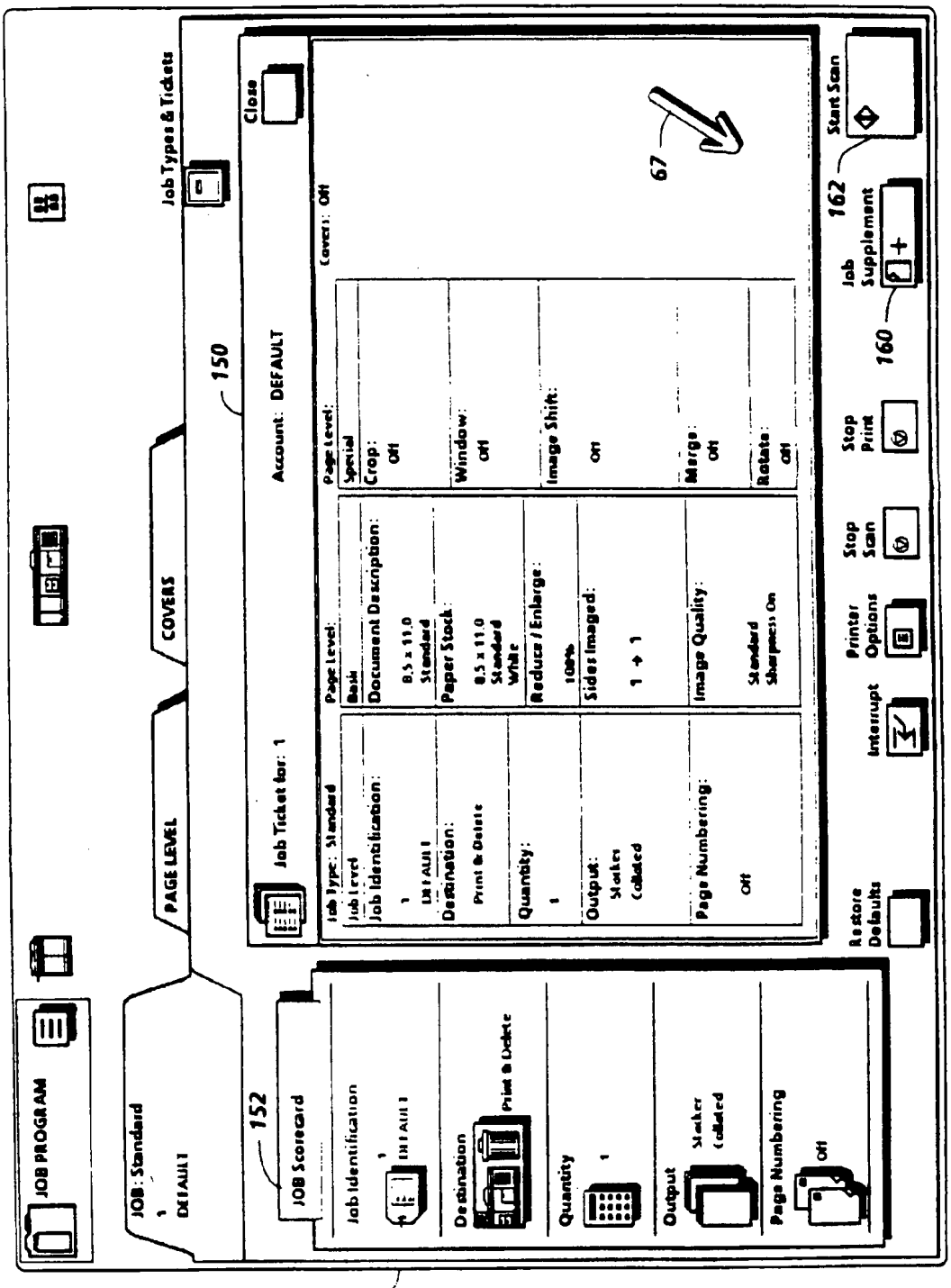

JOB PROGRAM
JOB : Standard
1
DEFAULT
PAGE LEVEL
COVERS
Job Types & Tickets
150
Job Ticket for: 1
Account: DEFAULT
Close
Job Type: Standard
Page Level:
Basic
Special
Job Level
Job Identification:
1
DEFAULT
Document Description:
8.5 x 11.0
Standard
Crop:
Off
Destination:
Print & Delete
Paper Stock:
8.5 x 11.0
Standard
White
Window:
Off
Quantity:
1
Reduce / Enlarge:
100%
Image Shift:
Output:
Stacker
Collated
Sides Imaged:
1 → 1
On
Page Numbering:
Off
Image Quality:
Standard
Sharpness On
Merge:
Off
Rotate:
Off
67
152
JOB Scorecard
Job Identification
1
DEFAULT
Destination
Print & Delete
Quantity
1
Output
Stacker
Collated
Page Numbering
Off
62
Restore Defaults
Interrupt
Printer Options
Stop Scan
Stop Print
160
Job Supplement
162
Start Scan

FIG. 7

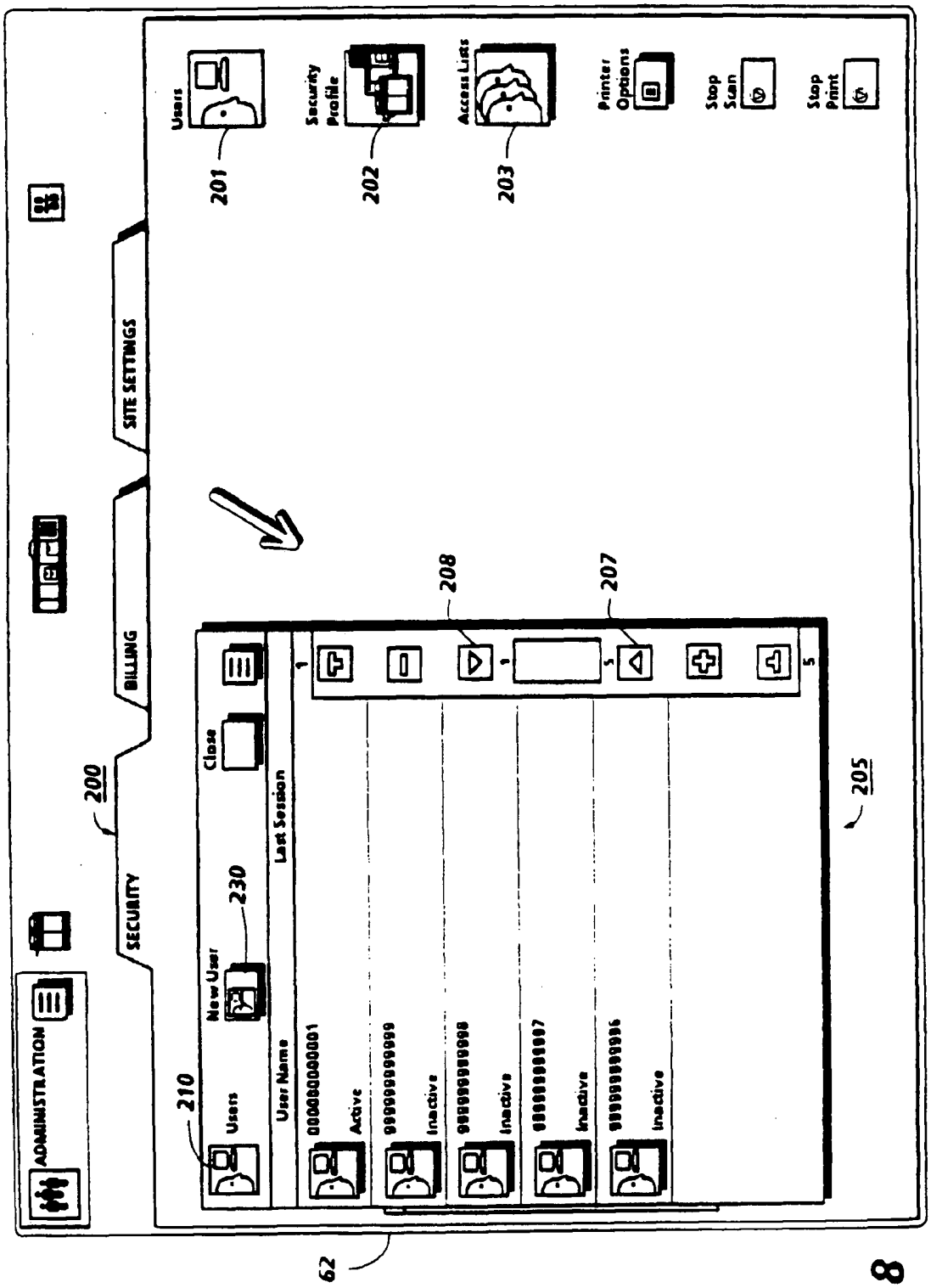

ADMINISTRATION
SECURITY
BILLING
SITE SETTINGS
200
Users
201
Security Profile
202
Access Lists
203
Printer Options
Stop Scan
Stop Print
208
207
205
Close
New User
230
Users
210
User Name
Last Session
000000000001
Active
999999999999
Inactive
999999999998
Inactive
999999999997
Inactive
999999999996
Inactive
62

FIG. 8

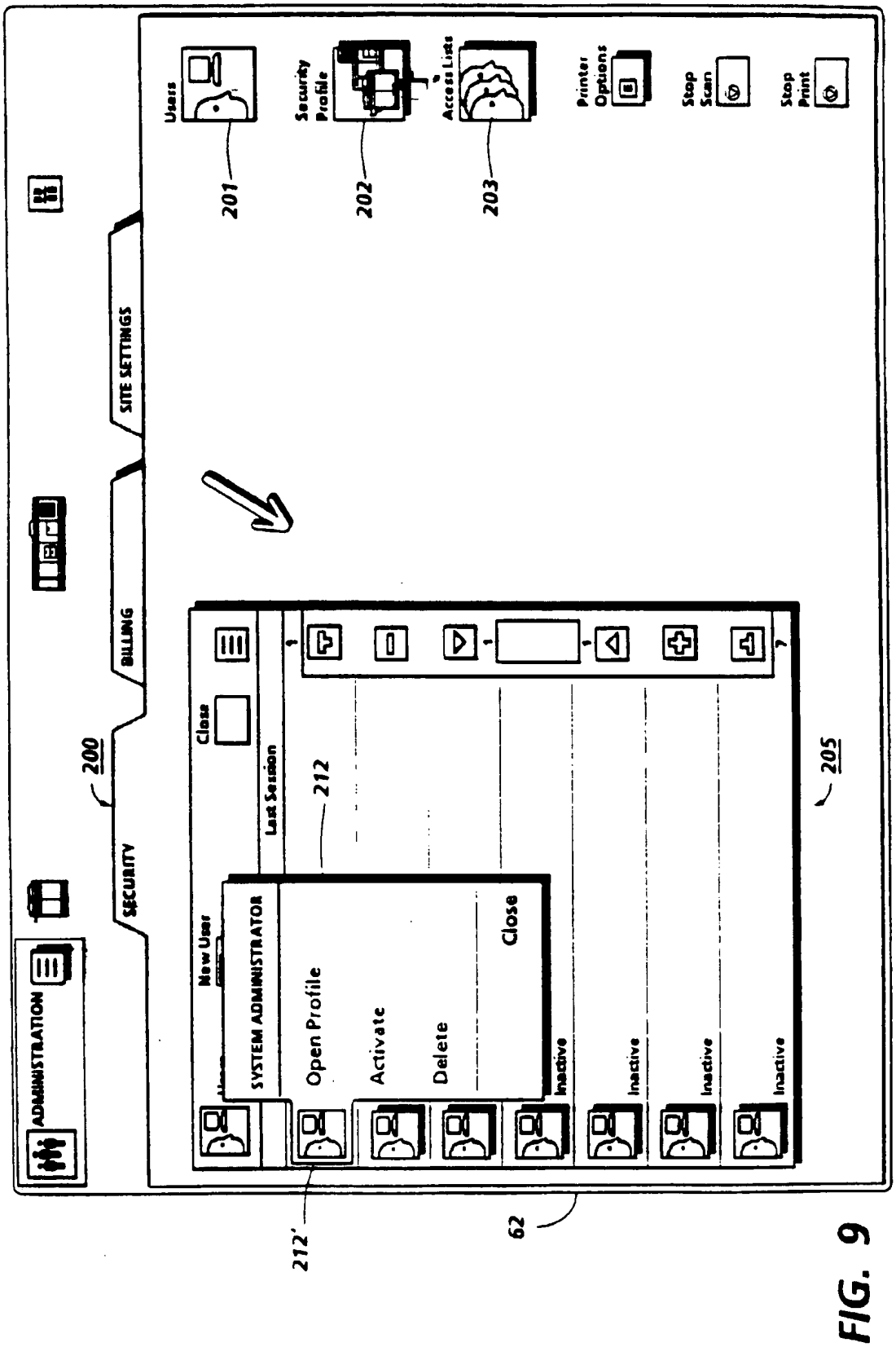

ADMINISTRATION
SECURITY
BILLING
SITE SETTINGS
200
Users
Security Profile
Access Lists
Printer Options
Stop Scan
Stop Print
201
202
203
Close
Last Session
212
205
New User
SYSTEM ADMINISTRATOR
Open Profile
Activate
Delete
Close
Inactive
212'
62

FIG. 9

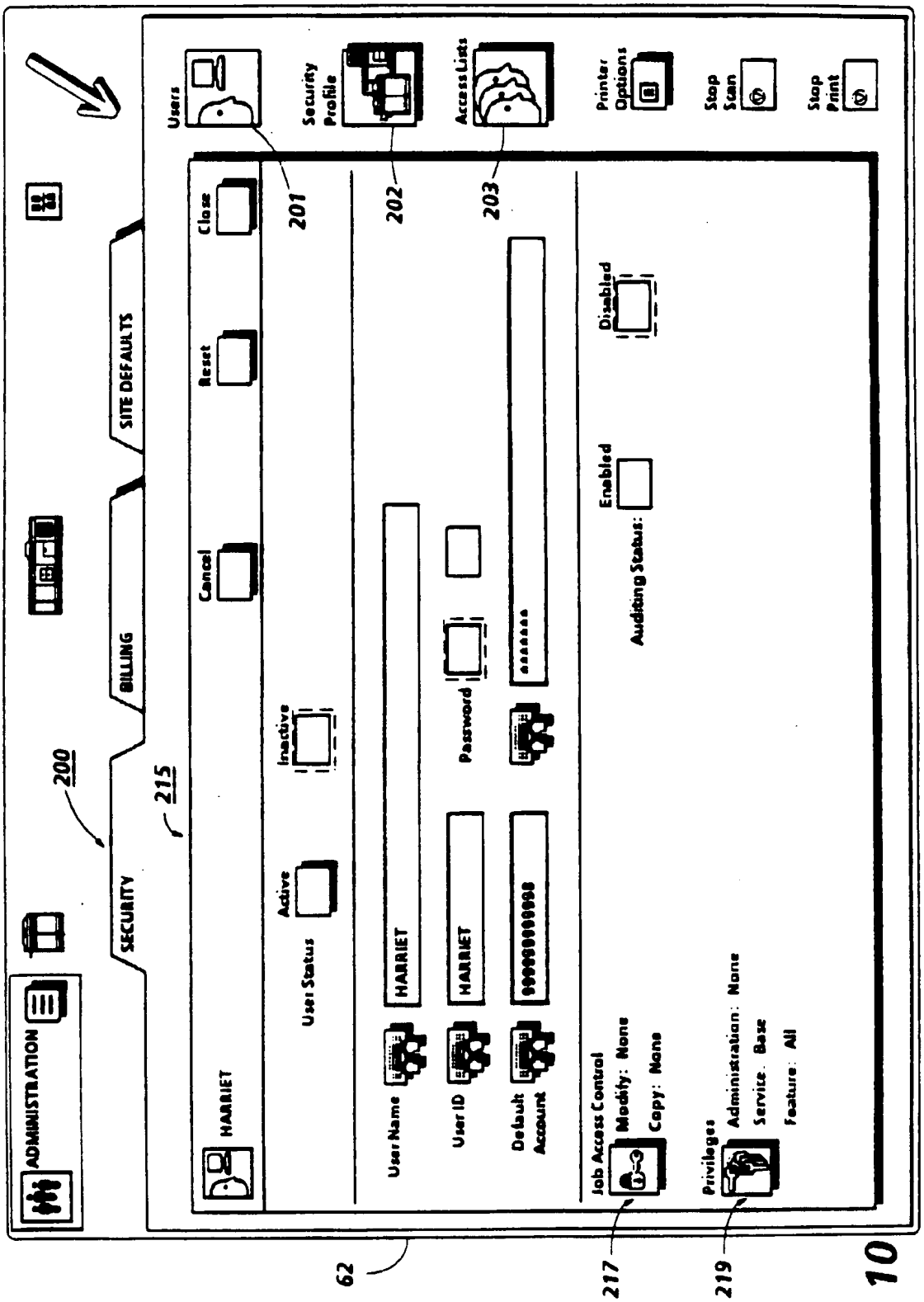

ADMINISTRATION
SECURITY
BILLING
SITE DEFAULTS
200
215
Users
Security Profile
Access Lists
Printer Options
Stop Scan
Stop Print
Close
Reset
Cancel
201
202
203
HARRIET
User Status
Active
Inactive
User Name
HARRIET
User ID
HARRIET
Password
Default Account
Enabled
Disabled
Auditing Status:
Job Access Control
Modify: None
Copy: None
Privileges
Administration: None
Service: Base
Feature: All
62
217
219

FIG. 10

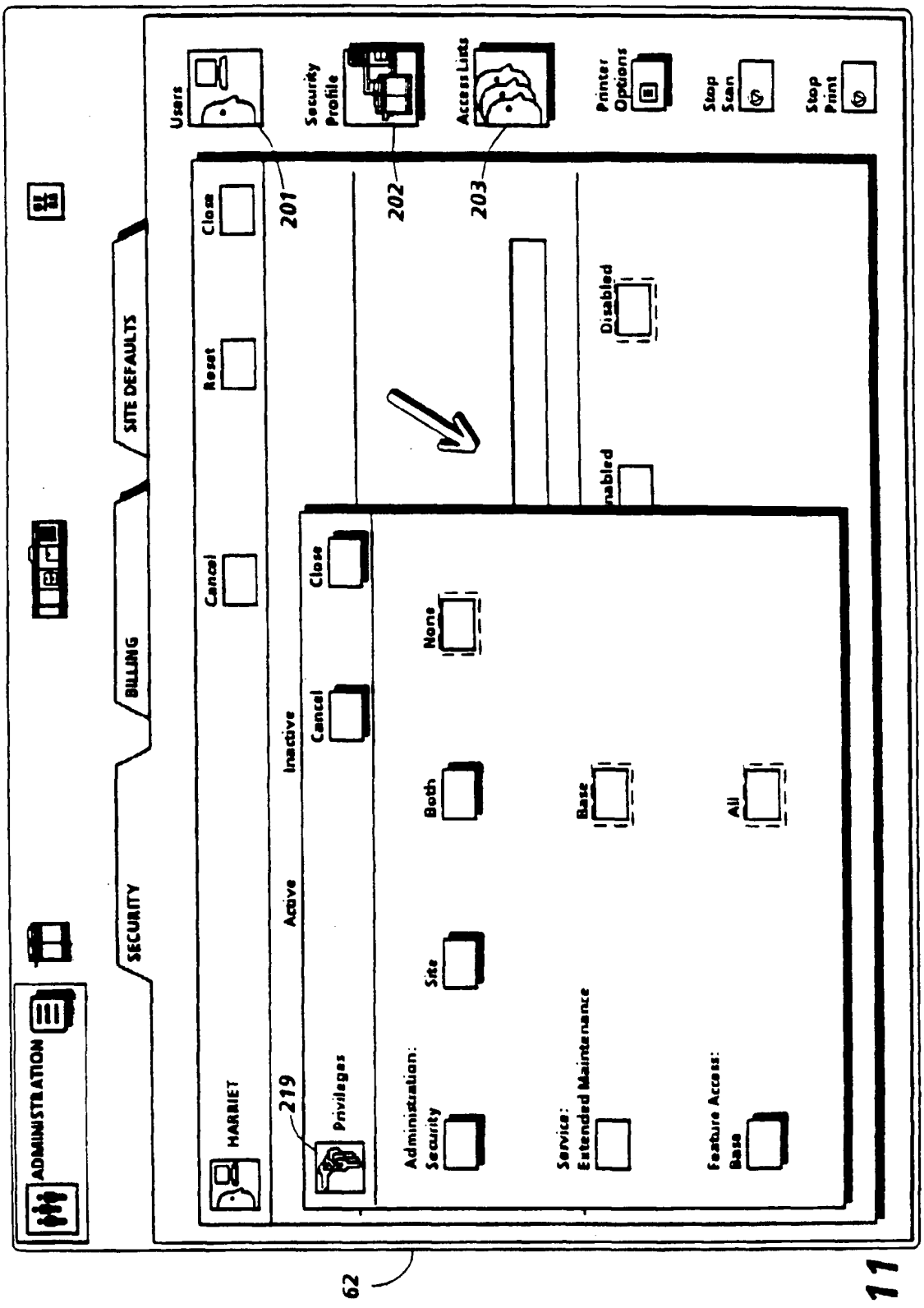

ADMINISTRATION
SECURITY
BILLING
SITE DEFAULTS
Users
Security Profile
Access Lists
Printer Options
Stop Scan
Stop Print
Close
Reset
Cancel
201
202
203
HARRIET
219
Privileges
Active
Inactive
Cancel
Close
Administration:
Security
Site
None
Both
Service:
Extended Maintenance
Base
Feature Access:
Base
All
Disabled
62

FIG. 11

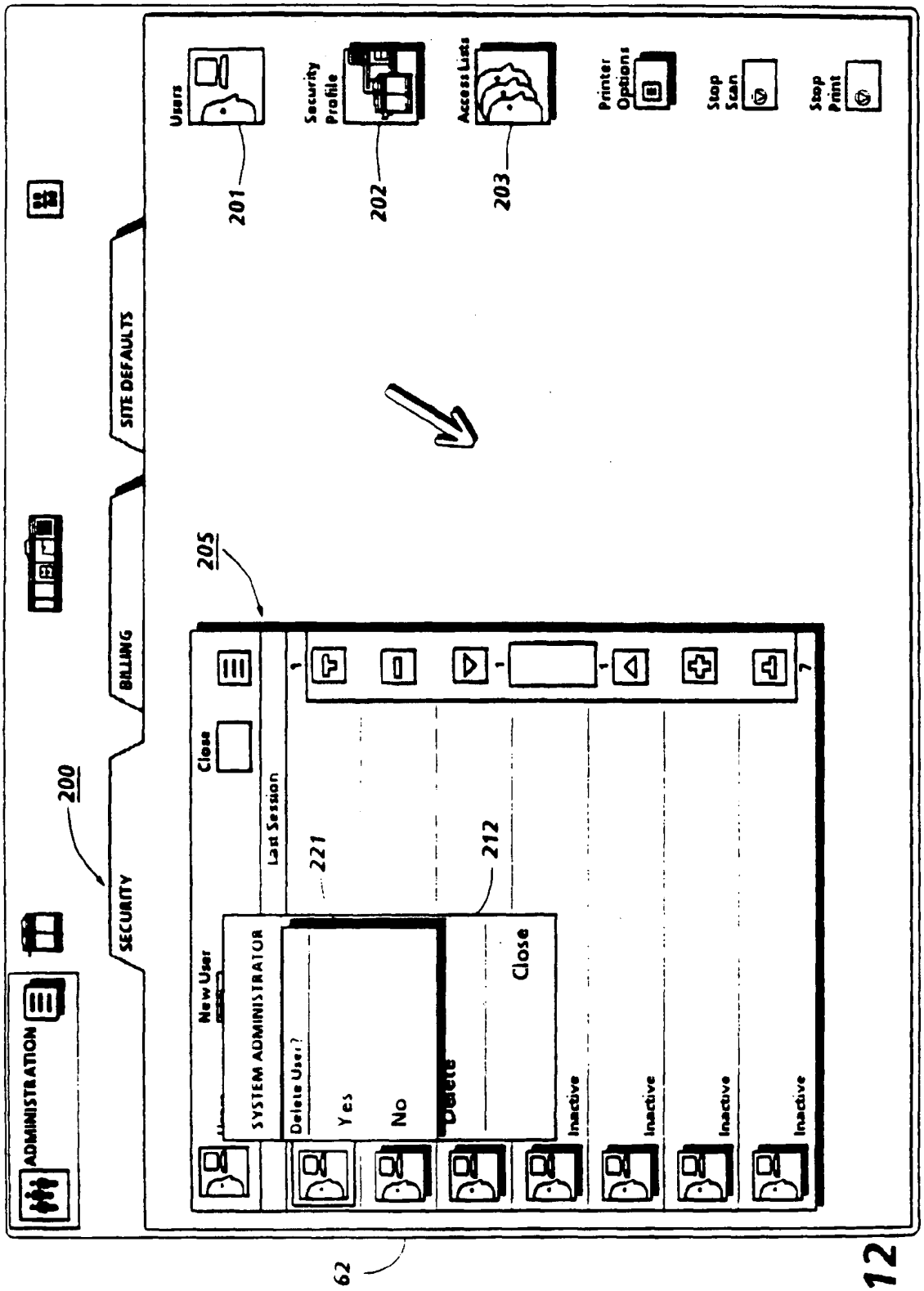

ADMINISTRATION
SECURITY
BILLING
SITE DEFAULTS
200
Users
Security Profile
Access Lists
Printer Options
Stop Scan
Stop Print
201
202
203
205
Close
Last Session
New User
SYSTEM ADMINISTRATOR
Delete User?
Yes
No
Delete
Close
221
212
Inactive
62

FIG. 12

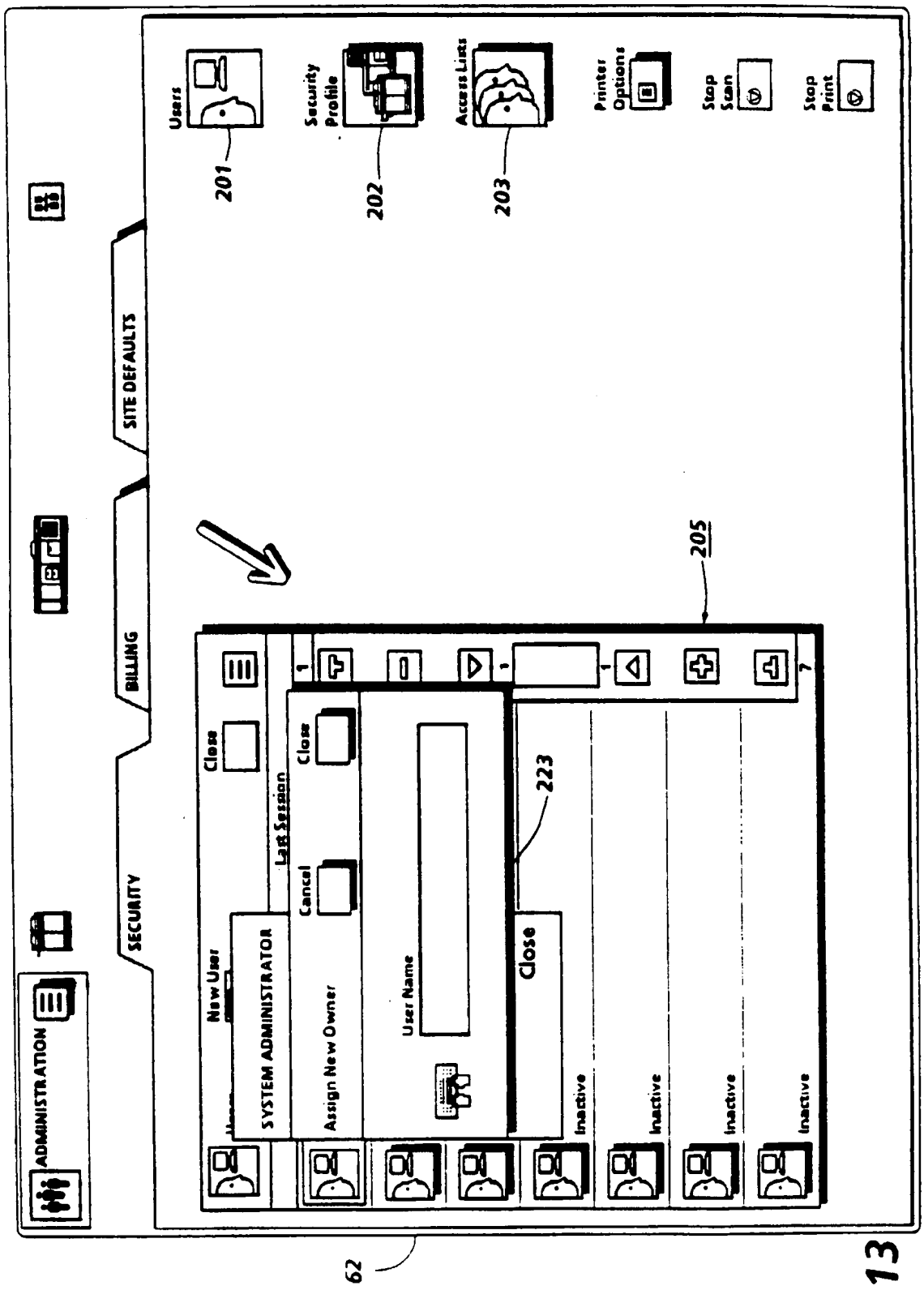

ADMINISTRATION
SECURITY
BILLING
SITE DEFAULTS
Users
Security Profile
Access Lists
Printer Options
Stop Scan
Stop Print
201
202
203
205
62
223
New User
SYSTEM ADMINISTRATOR
Last Session
Close
Cancel
Assign New Owner
User Name
Close
Inactive
Inactive
Inactive
Inactive

FIG. 13

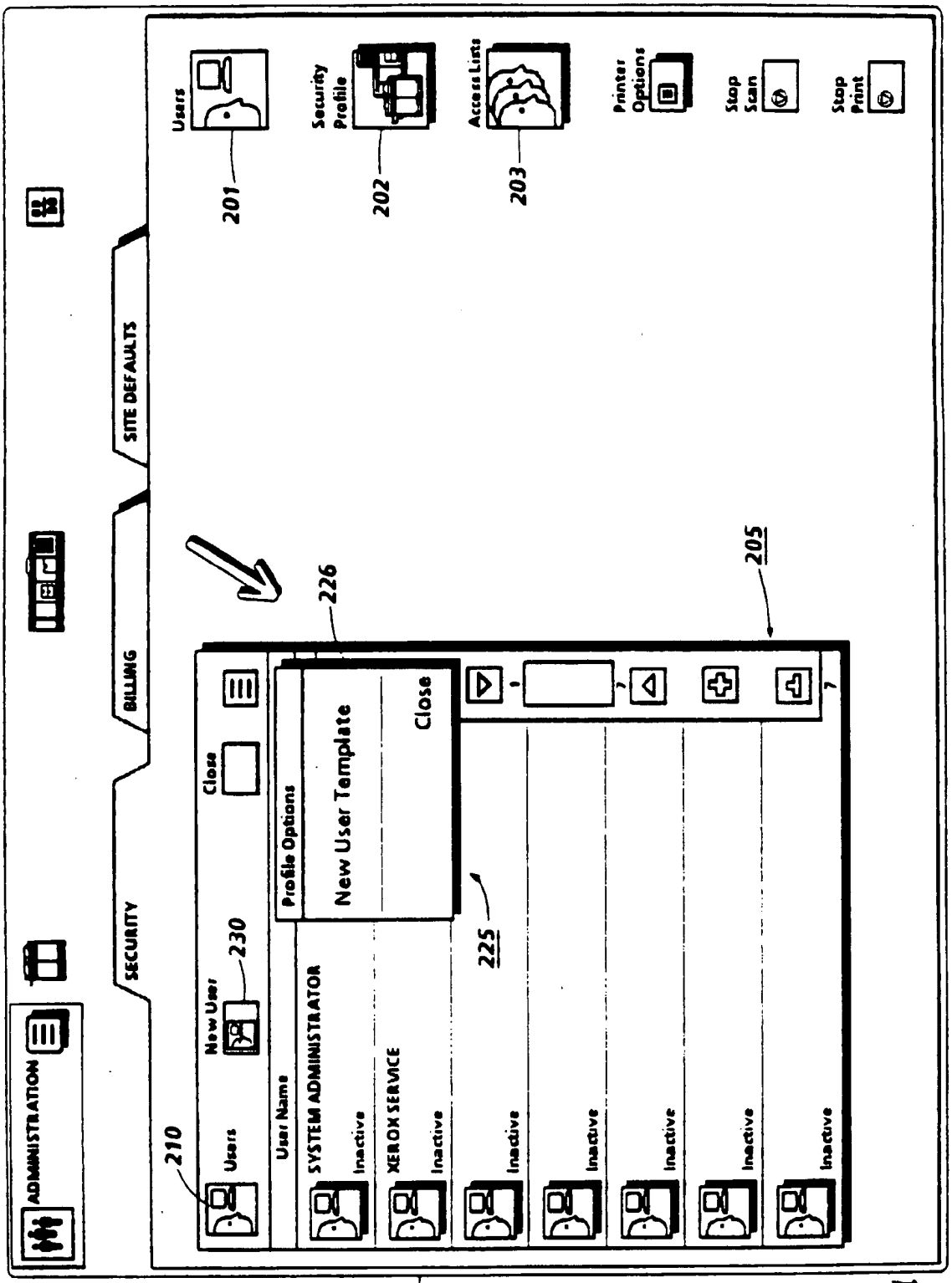

ADMINISTRATION
SECURITY
BILLING
SITE DEFAULTS
Users
201
Security Profile
202
Access Lists
203
Printer Options
Stop Scan
Stop Print
205
226
New User
230
Close
Profile Options
New User Template
Close
225
User Name
SYSTEM ADMINISTRATOR
XEROX SERVICE
Inactive
210
62

FIG. 14

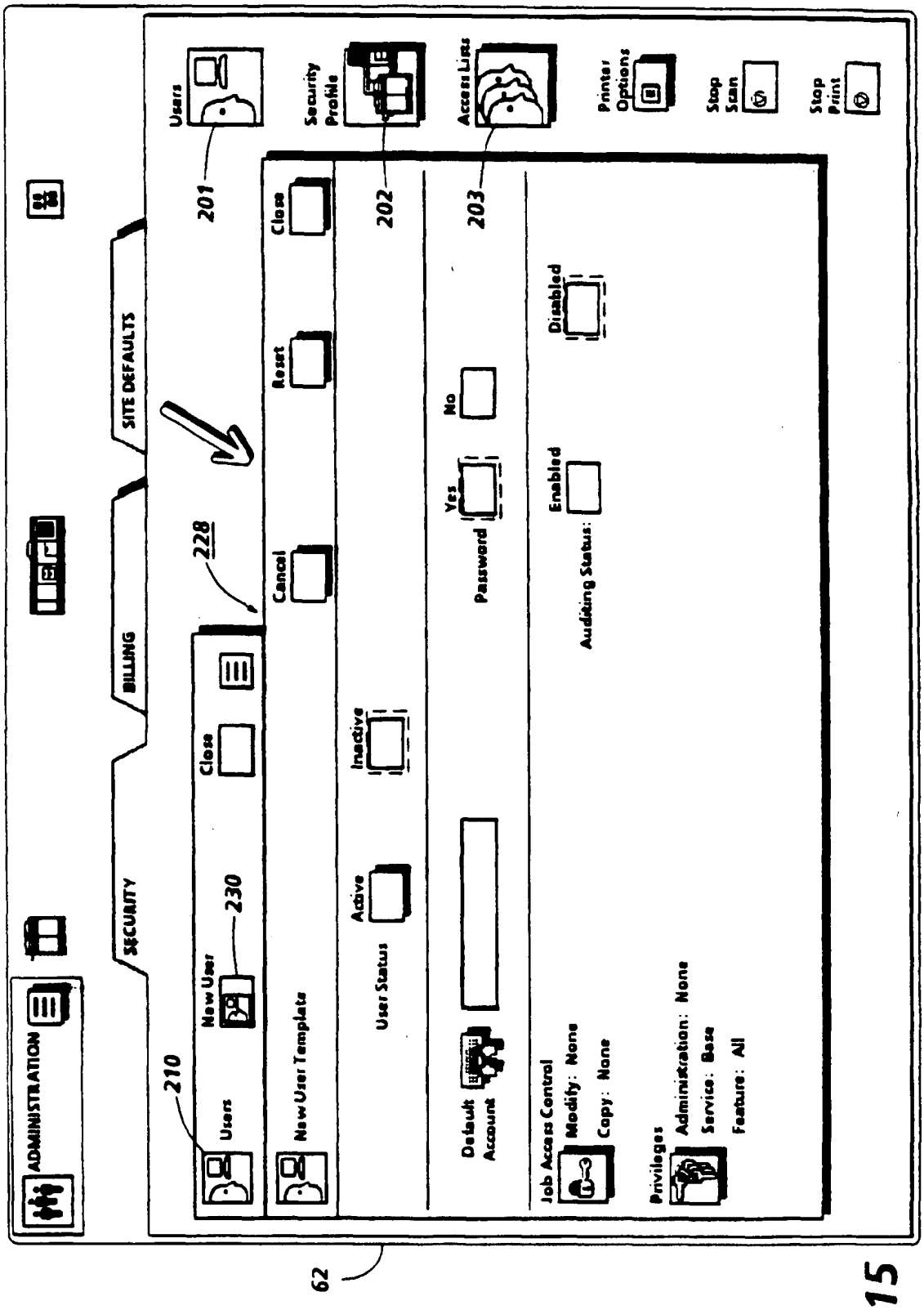

ADMINISTRATION
SECURITY
BILLING
SITE DEFAULTS
Users
Security Profile
Access Lists
Printer Options
Stop Scan
Stop Print
201
202
203
210
228
230
62
Close
Reset
Cancel
New User
Close
Inactive
Active
User Status
Yes
No
Password
Enabled
Disabled
Auditing Status:
Default Account
New User Template
Job Access Control
Modify: None
Copy: None
Privileges
Administration: None
Service: Base
Feature: All

FIG. 15

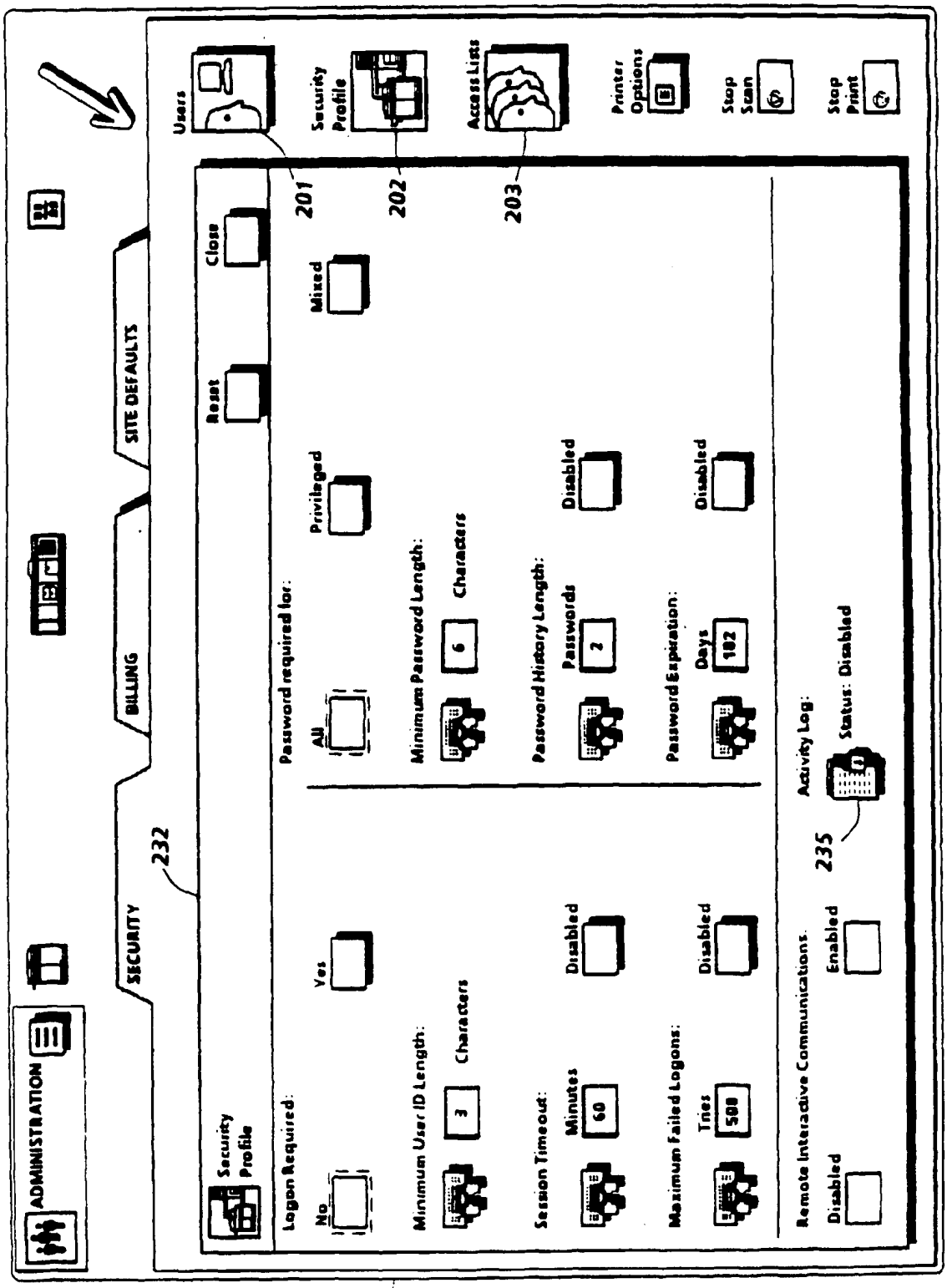

ADMINISTRATION
SECURITY
BILLING
SITE DEFAULTS
232
62
Users
Security Profile
Access Lists
Printer Options
Stop Scan
Stop Print
201
202
203
Close
Reset
Security Profile
Logon Required:
No
Yes
Password required for:
All
Mixed
Privileged
Minimum User ID Length:
3
Characters
Minimum Password Length:
6
Characters
Session Timeout:
Minutes
60
Disabled
Password History Length:
Passwords
2
Disabled
Maximum Failed Logons:
Tries
500
Disabled
Password Expiration:
Days
182
Disabled
Remote Interactive Communications:
Disabled
Enabled
235
Activity Log:
Status: Disabled

FIG. 16

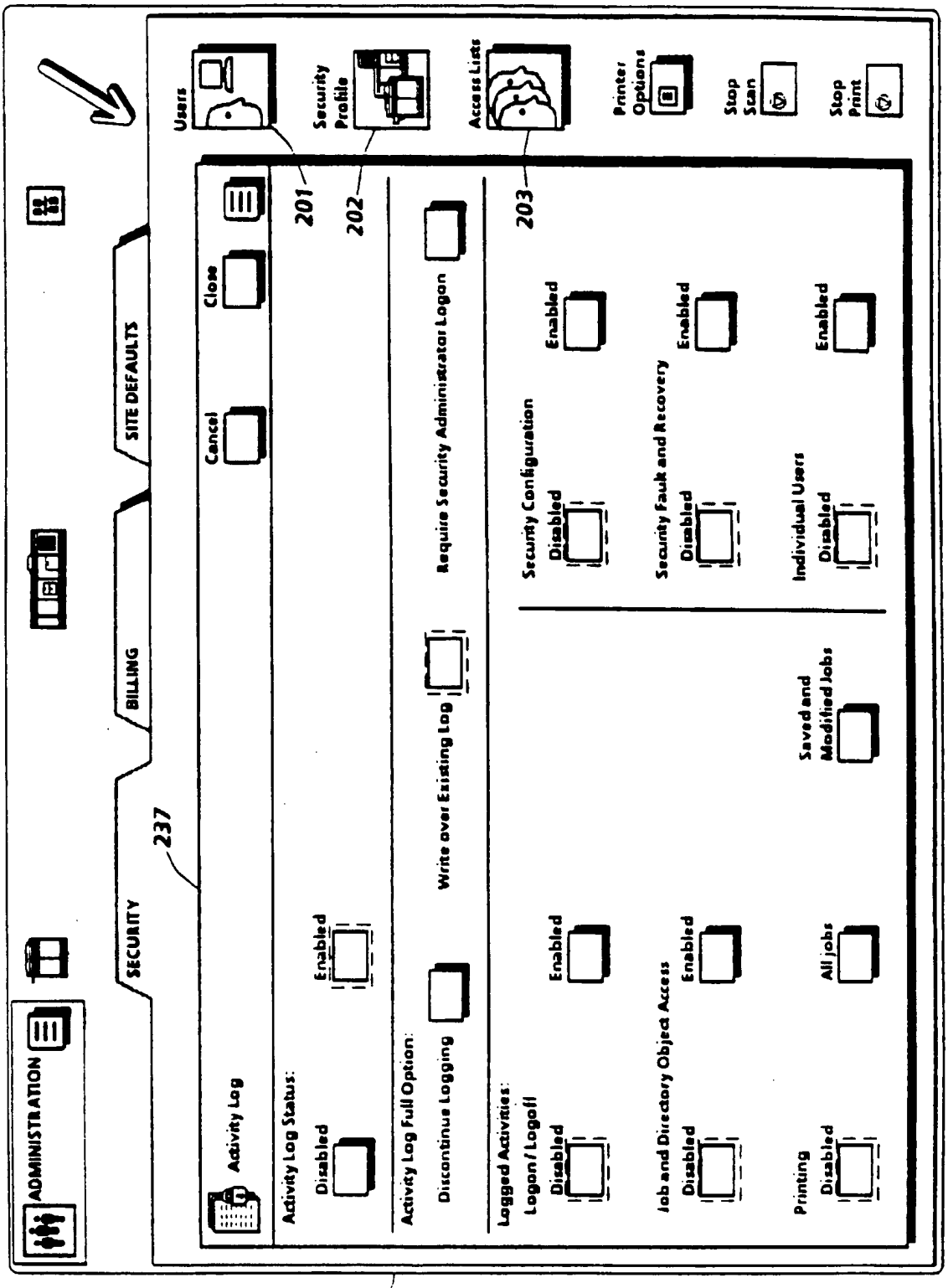

ADMINISTRATION
SECURITY
BILLING
SITE DEFAULTS
237
62
Users
Security Profile
Access Lists
Printer Options
Stop Scan
Stop Print
201
202
203
Activity Log
Cancel
Close
Activity Log Status:
Disabled
Enabled
Activity Log Full Option:
Discontinue Logging
Write over Existing Log
Require Security Administrator Logon
Logged Activities:
Logon / Logoff
Disabled
Enabled
Job and Directory Object Access
Disabled
Enabled
Printing
Disabled
All jobs
Saved and Modified Jobs
Security Configuration
Disabled
Enabled
Security Fault and Recovery
Disabled
Enabled
Individual Users
Disabled
Enabled

FIG. 17

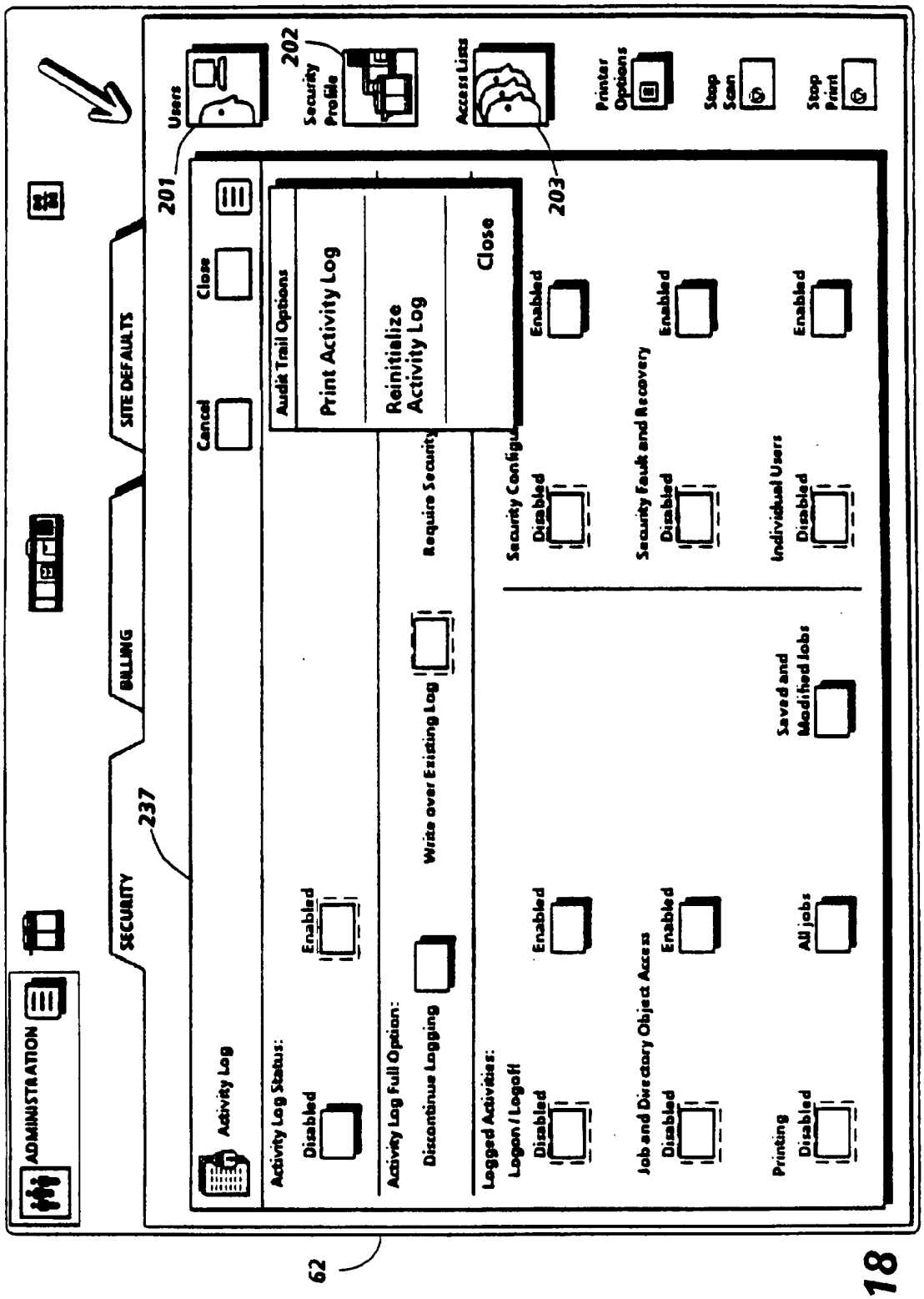

ADMINISTRATION
SECURITY
237
BILLING
SITE DEFAULTS
201
Users
202
Security Profile
Access Lists
Printer Options
Stop Scan
Stop Print
Activity Log
Cancel
Close
Audit Trail Options
Print Activity Log
Reinitialize Activity Log
Close
203
Activity Log Status:
Disabled
Enabled
Activity Log Full Option:
Discontinue Logging
Write over Existing Log
Require Security
Logged Activities:
Logon / Logoff
Disabled
Enabled
Job and Directory Object Access
Disabled
Enabled
Printing
Disabled
All jobs
Saved and Modified Jobs
Security Configu
Disabled
Enabled
Security Fault and Recovery
Disabled
Enabled
Individual Users
Disabled
Enabled
62

FIG. 18

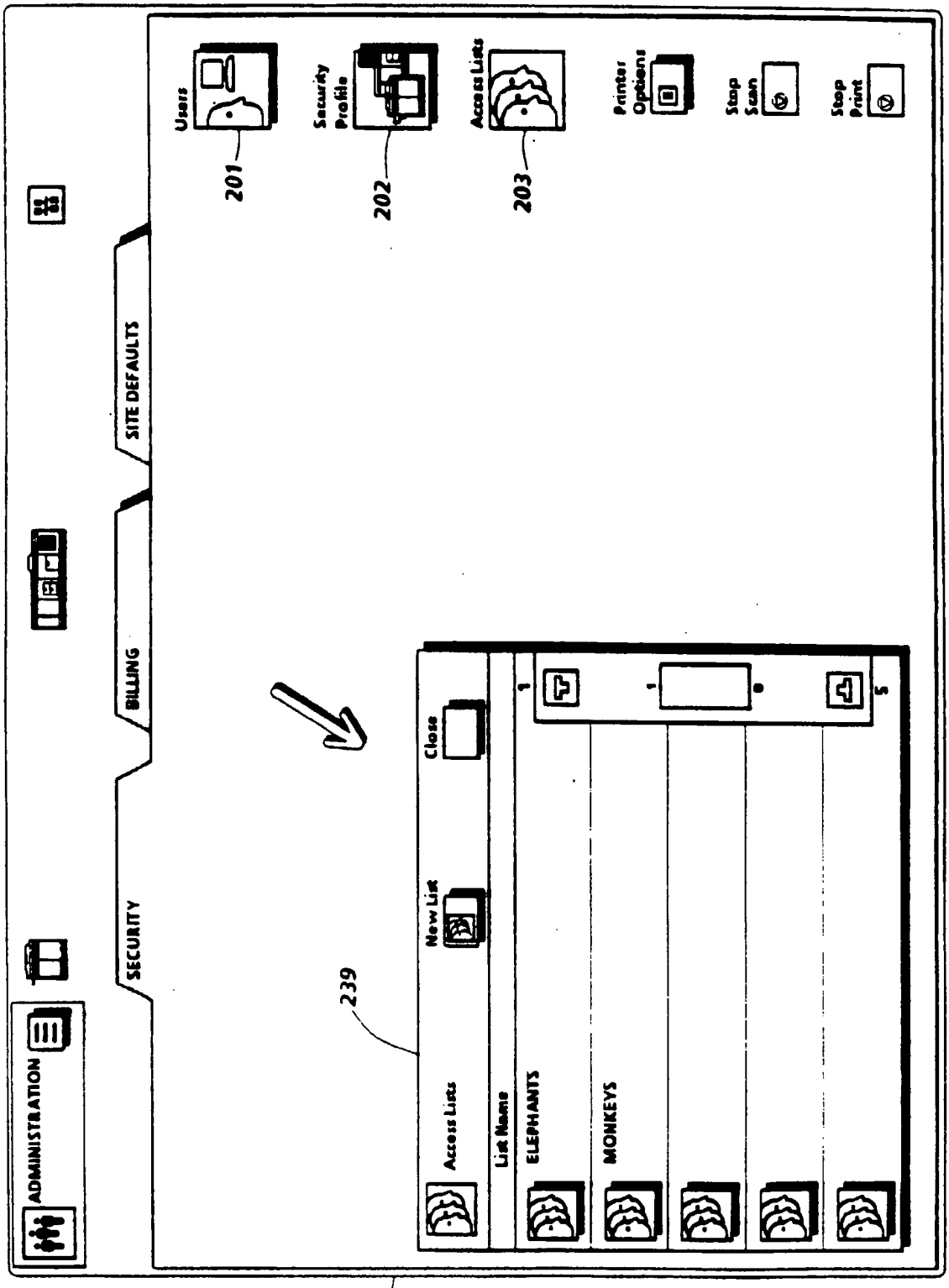

ADMINISTRATION
SECURITY
BILLING
SITE DEFAULTS
Users
Security Profile
Access Lists
Printer Options
Stop Scan
Stop Print
201
202
203
239
62
New List
Close
Access Lists
List Name
ELEPHANTS
MONKEYS

FIG. 19

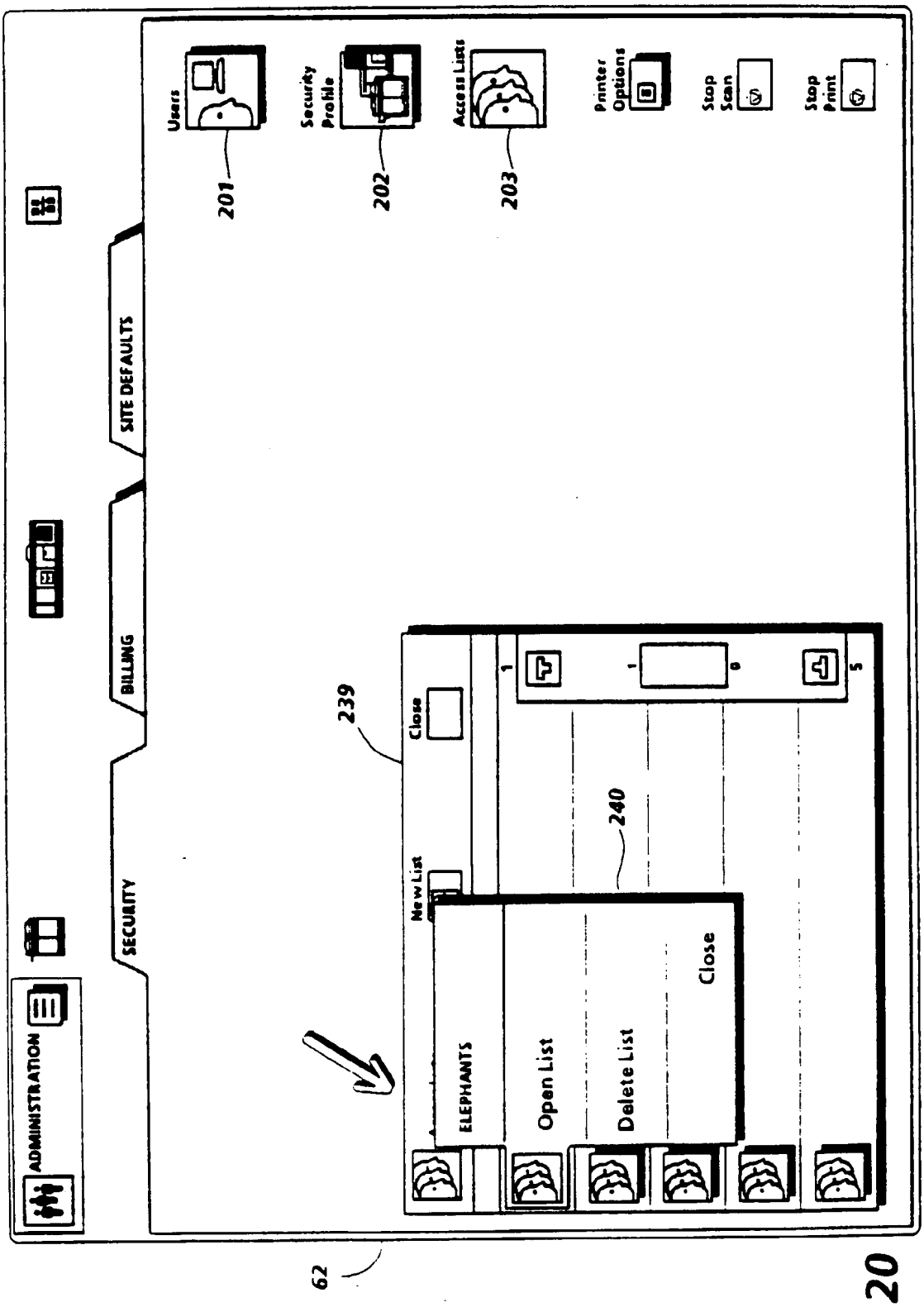

ADMINISTRATION
SECURITY
BILLING
SITE DEFAULTS
Users
Security Profile
Access Lists
Printer Options
Stop Scan
Stop Print
201
202
203
239
240
62
Close
New List
ELEPHANTS
Open List
Delete List
Close

FIG. 20

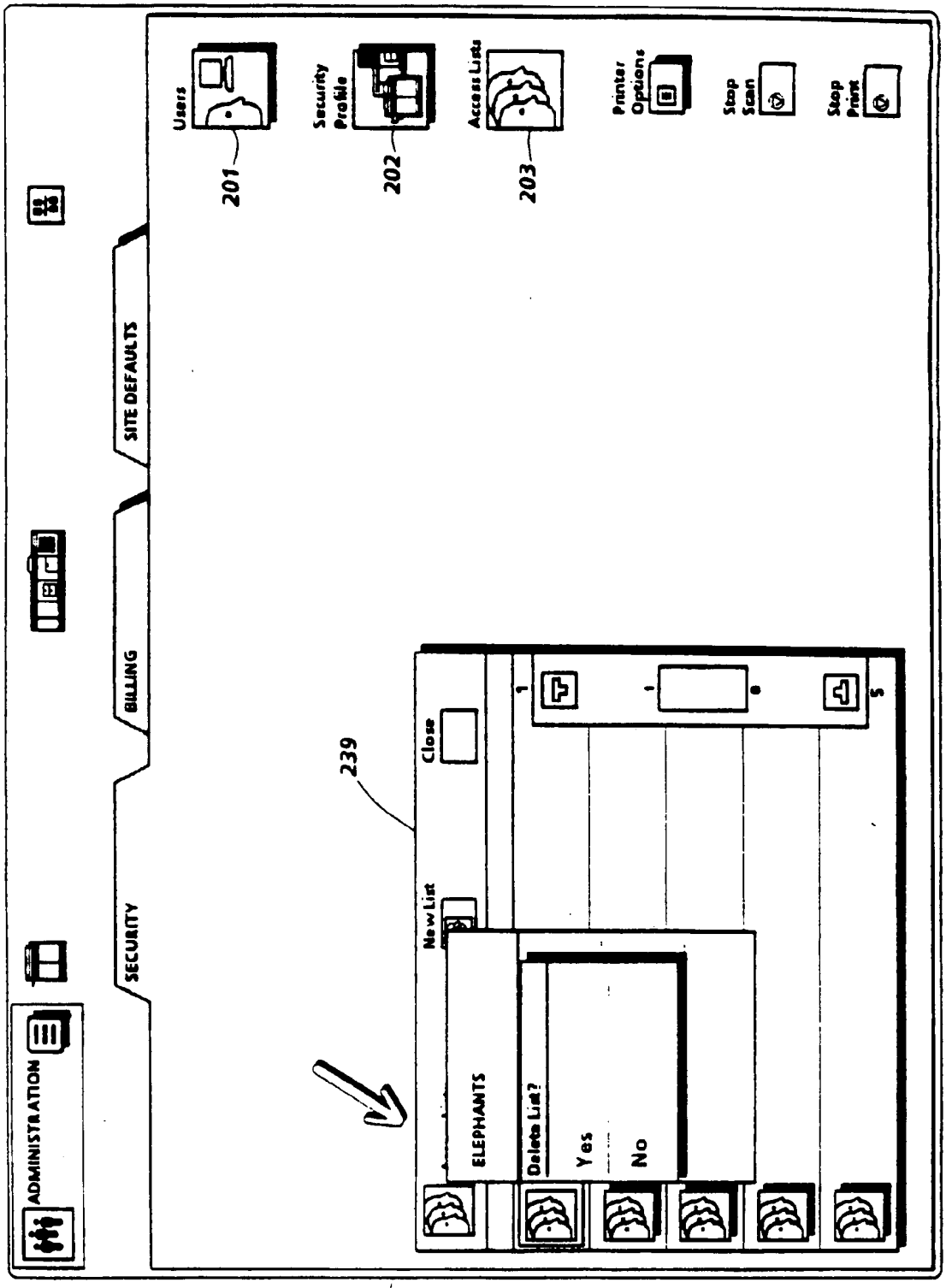

ADMINISTRATION
SECURITY
BILLING
SITE DEFAULTS
Users
Security Profile
Access Lists
Printer Options
Stop Scan
Stop Print
201
202
203
239
62
Close
New List
ELEPHANTS
Delete List?
Yes
No

FIG. 21

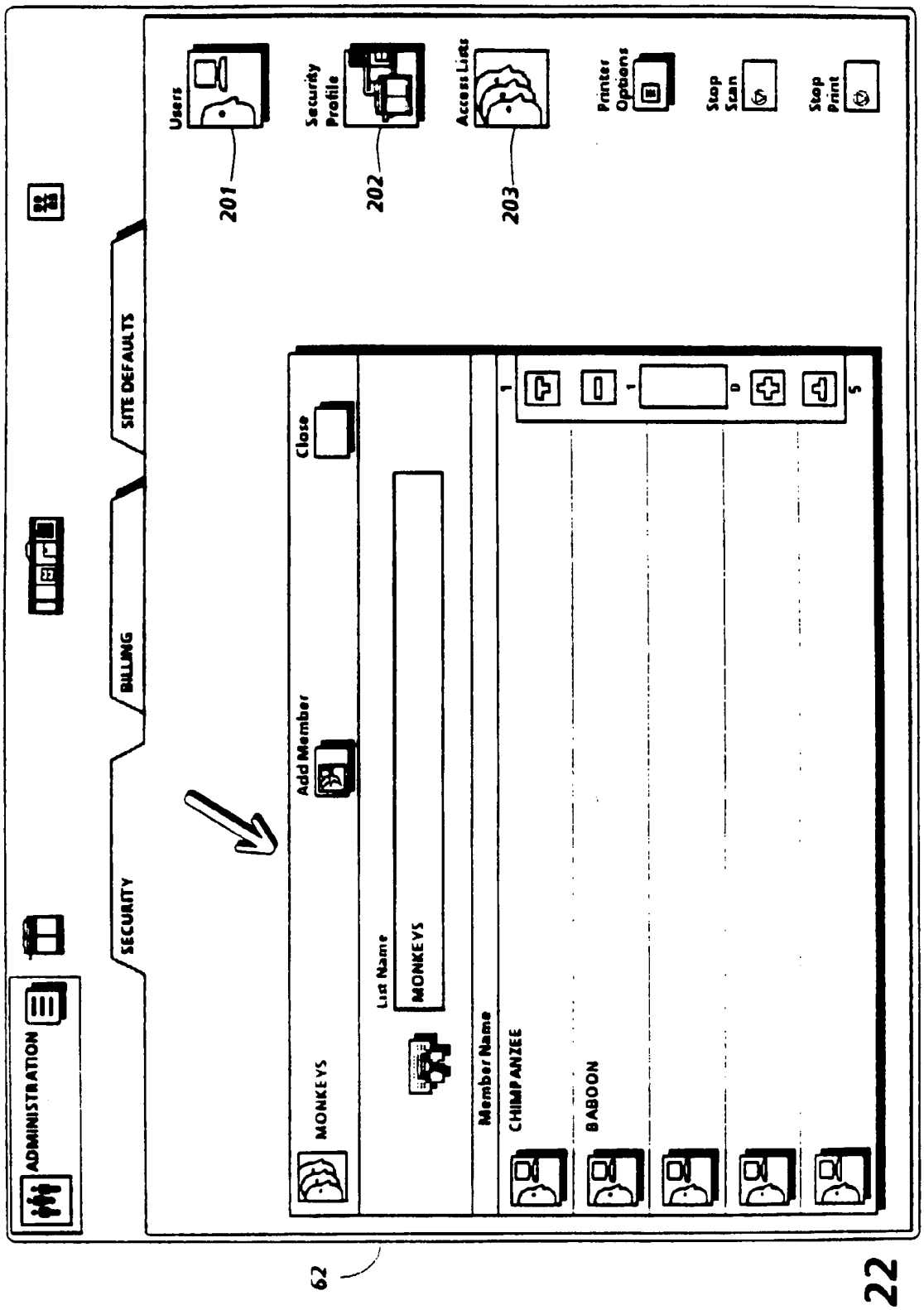

ADMINISTRATION
SECURITY
BILLING
SITE DEFAULTS
Users
201
Security Profile
202
Access Lists
203
Printer Options
Stop Scan
Stop Print
Close
Add Member
List Name
MONKEYS
MONKEYS
Member Name
CHIMPANZEE
BABOON
62

FIG. 22

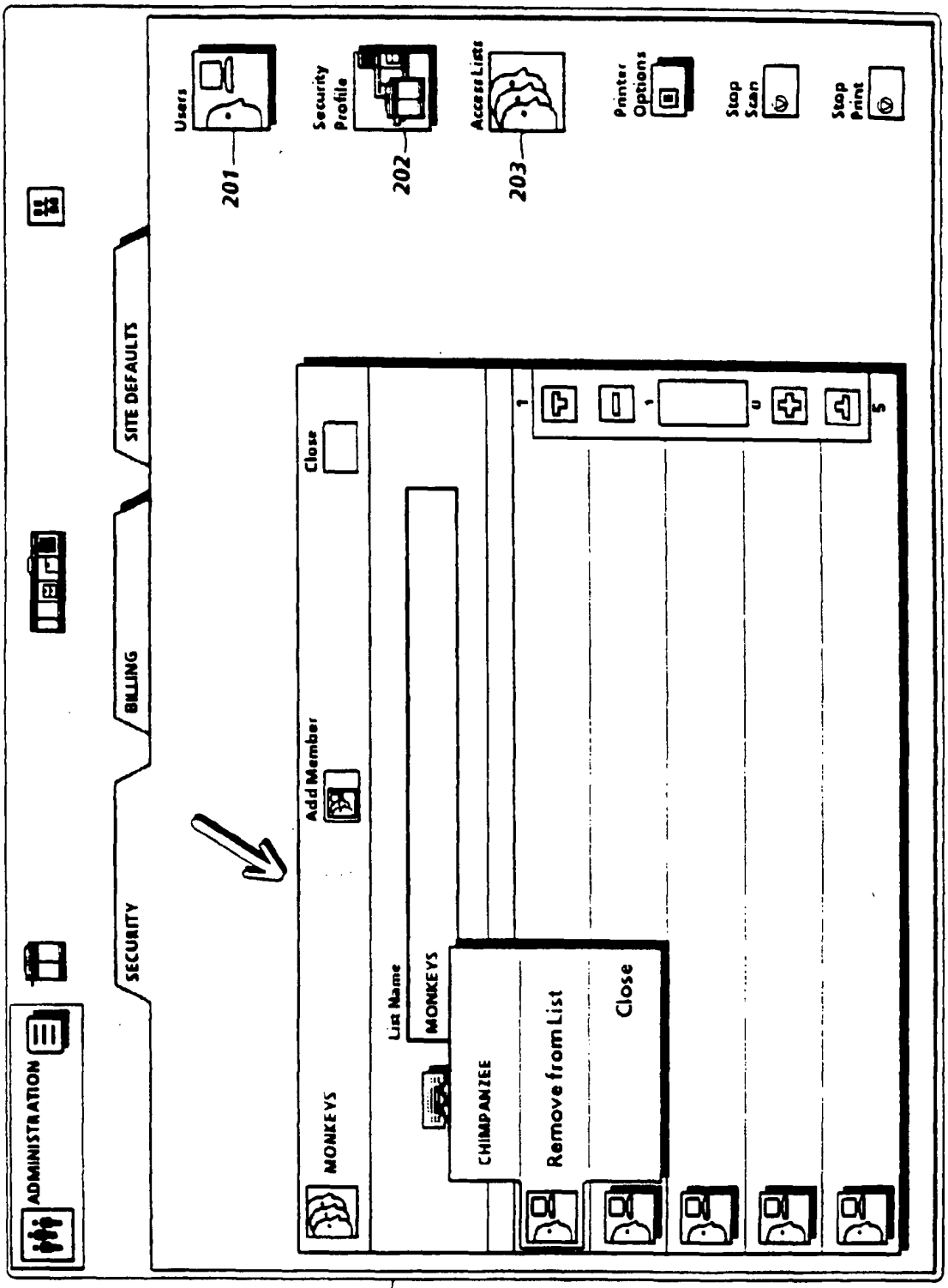

ADMINISTRATION
SECURITY
BILLING
SITE DEFAULTS
Users
Security Profile
Access Lists
Printer Options
Stop Scan
Stop Print
201
202
203
Close
Add Member
List Name
MONKEYS
MONKEYS
CHIMPANZEE
Remove from List
Close
62

FIG. 23

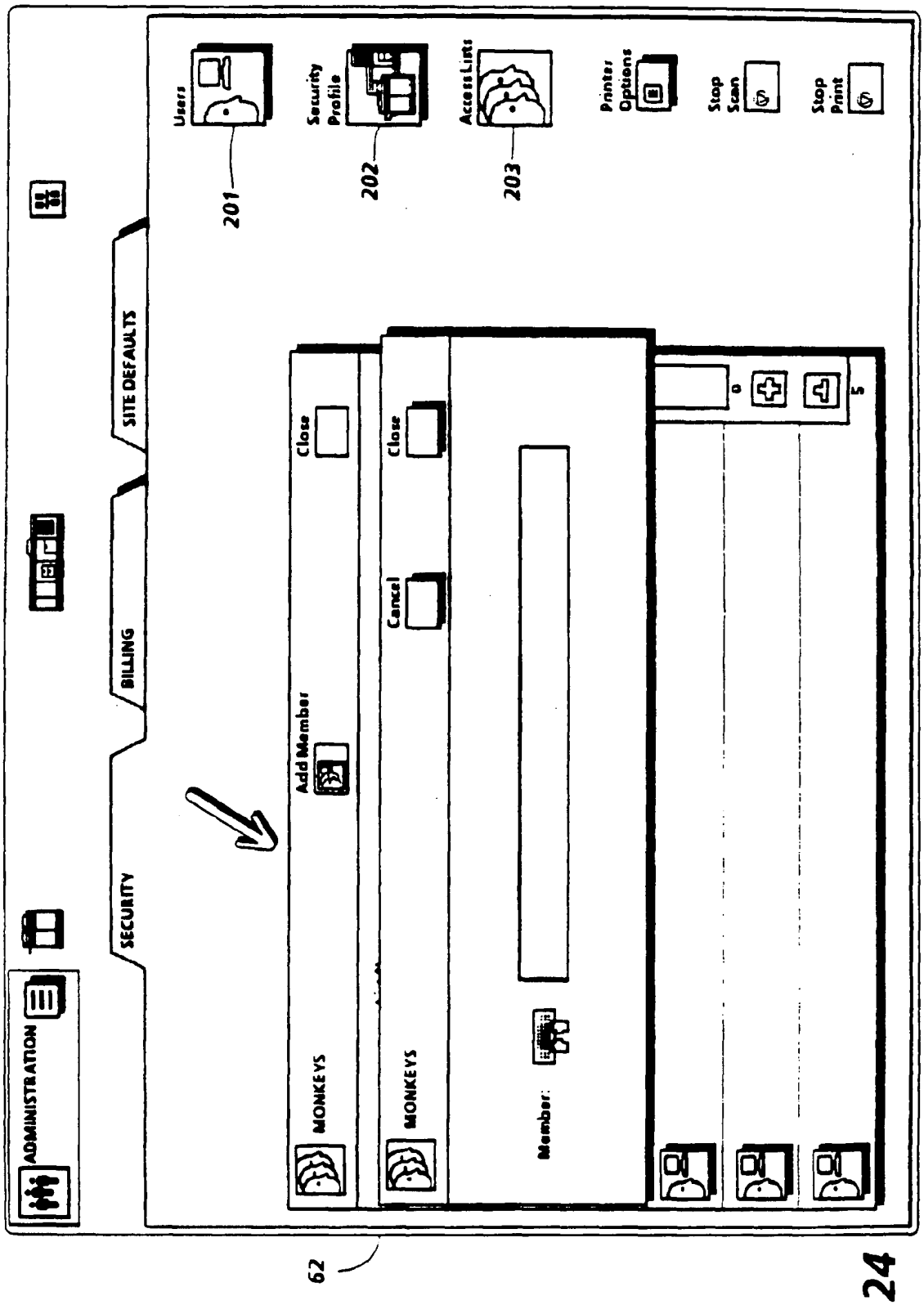

ADMINISTRATION
SECURITY
BILLING
SITE DEFAULTS
Users
Security Profile
Access Lists
Printer Options
Stop Scan
Stop Print
201
202
203
Add Member
Close
Cancel
MONKEYS
Member:
62

FIG. 24

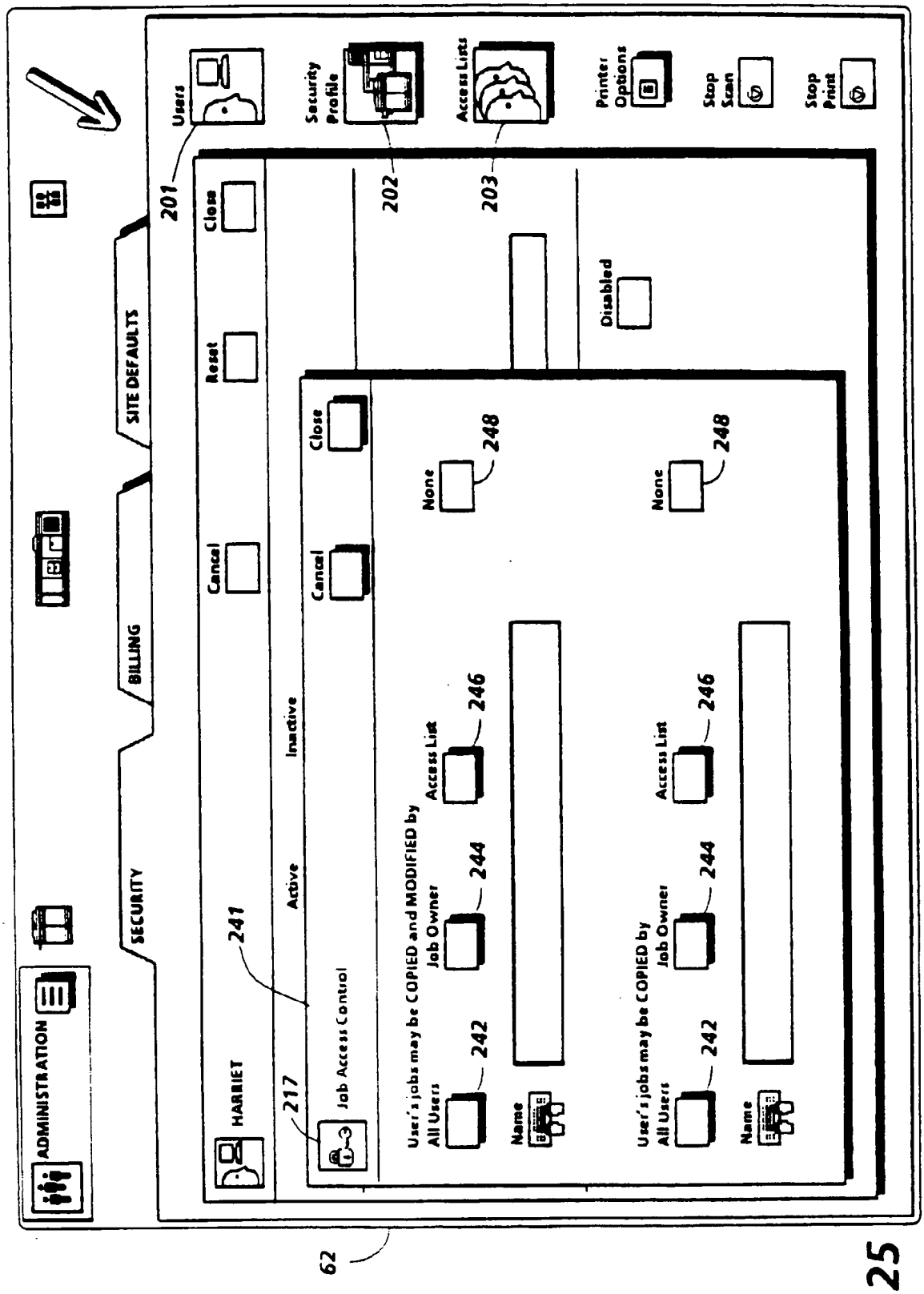

ADMINISTRATION
SECURITY
BILLING
SITE DEFAULTS
Users
Security Profile
Access Lists
Printer Options
Stop Scan
Stop Print
201
202
203
Close
Reset
Cancel
Close
Cancel
Disabled
HARRIET
241
Active
Inactive
217
Job Access Control
User's jobs may be COPIED and MODIFIED by
All Users
242
Job Owner
244
Access List
246
None
248
Name
User's jobs may be COPIED by
All Users
242
Job Owner
244
Access List
246
None
248
Name
62

FIG. 25

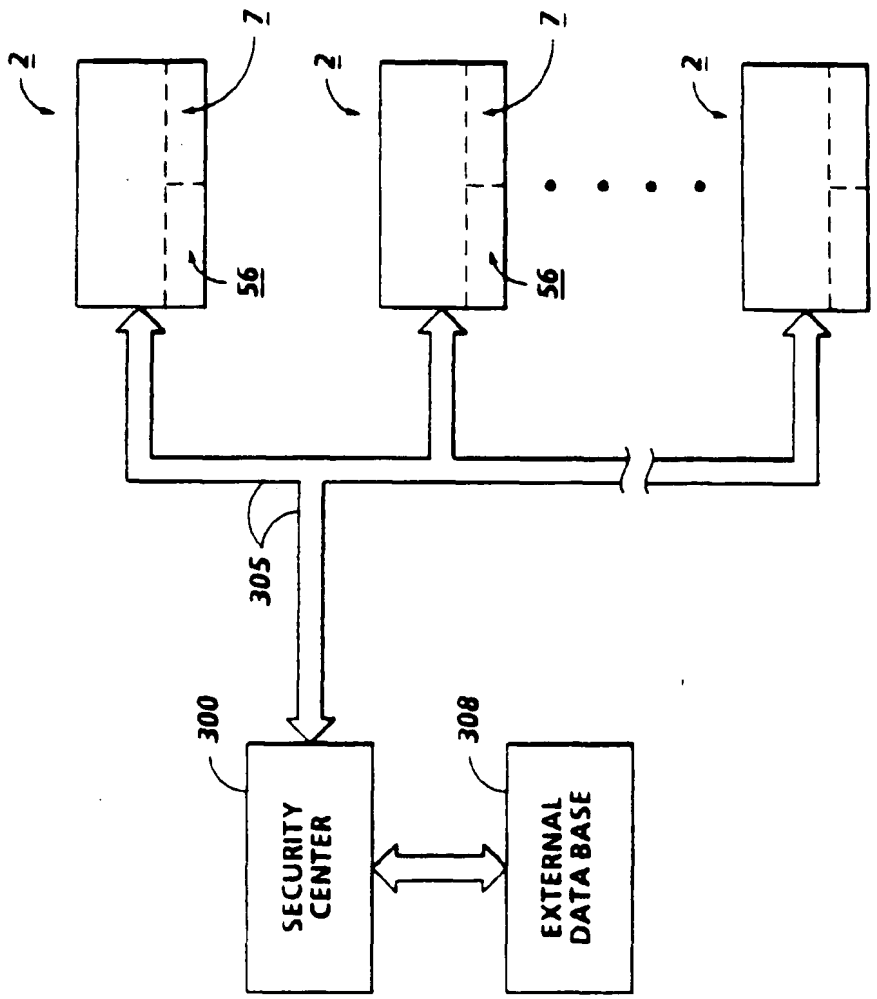


FIG. 26